HY-LINE®
SYSTEMS GMBH

M2M Industrie Router

Benutzerhandbuch

truecon®

20 YEARS HY-LINE

Firewall – VPN – RS-232 over Ethernet
Alarm SMS / E-Mail – Web-Server

Urheberrecht

Copyright 2013 ***Handbuch Version R1.9.2a – 29.09.2015***
Für diese Dokumentation behalten wir uns alle Rechte vor. Dazu zählen insbesondere die fotomechanische Wiedergabe und die Speicherung in elektronischen Medien. In der Dokumentation verwendete Warenbezeichnungen und Firmennamen unterliegen den Rechten der jeweils betroffenen Firmen.

Technische Änderungen
HY-LINE behält sich vor, Änderungen zu Darstellungen und Angaben, in dieser Dokumentation, ohne vorherige Ankündigungen vorzunehmen. Diese Dokumentation wurde mit größter Sorgfalt erstellt und wird regelmäßig überarbeitet. Trotz aller Kontrollen ist es jedoch nicht auszuschließen, dass technische Ungenauigkeiten und typografische Fehler übersehen wurden. Alle uns bekannten Fehler werden bei neuen Auflagen beseitigt. Für Hinweise auf Fehler in dieser Dokumentation sind wir jederzeit dankbar.

Support
Wir stellen Ihnen auf unseren Internetseiten www.hy-line.de einen umfangreichen Supportbereich zur Verfügung. Dort finden Sie neueste Beschreibungen und Datenblätter. Außerdem finden Sie auf www.hy-line.de eine Datenbank mit einer Vielzahl an Fragen und Antworten rund um die truecon Produktfamilie. Sollten Sie weitere Fragen haben oder Hilfestellung benötigen, können Sie Ihre Supportanfragen auch an systems@hy-line.de richten.

Pflegehinweise
Wischen Sie das Gehäuse nur mit einem trockenen Tuch, ohne Zusatz von Wasser oder chemischen Stoffen ab. Setzen Sie dieses Produkt niemals Spritzwasser aus.

Sicherheitshinweis
Öffnen Sie niemals das Gehäuse des Routers bei angeschlossener Spannungsversorgung. Die Spannungsversorgung muß immer direkt am Gerät abgezogen werden vor Öffnen des Gerätes. Es besteht die Gefahr eines Stromschlags.

IBM PC, AT, XT sind Warenzeichen von International Business Machine Corporation.

Windows™ ist ein Warenzeichen von Microsoft Corporation.
Java ist ein Warenzeichen von Oracle Corporation.
Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

Allgemein: Technische Änderungen und Irrtümer vorbehalten.

Entsorgung nach WEEE

Serviceadressen und Lieferanten von Zubehör- und Ersatzteilen:

HY-LINE Systems GmbH
Inselkammerstr. 10
82008 Unterhaching

Tel +49 (0)89/ 61450381
Fax +49 (0)89/ 61450385

E-Mail systems@hy-line.de
Internet: www.hy-line.de/systems
M2M-Router: www.hy-line.de/router

Inhaltsverzeichnis

Produktbeschreibung 4
Sicherheitsbestimmungen 5
Router Varianten 7
Anzeige- und Bedienelemente 8

Inbetriebnahme / Schnellanleitung 9
Softwarereset (Auslieferungszustand) 10
Konfiguration - Home 11
Base Settings
- Identification 14
- Network 16
- Date & Time 19

Connection Settings
- Phone Settings 20
- Internet Settings 21
- Dial-In / Call back 23

E-Mail 25
I/O-Settings Input / Output 27
Firewall 29
NAT 31
Services – Status 32
- DHCP/DNS Server 33
- DynDNS 34
- InetWD + Redundancy 35
- NTPd 39
- Ser2TCP 40
- SNMP 41
- SShd 42
- Syslogd 43
- FTP Server 43
- UDP-Broadcast 44
- Webserver 45
- VPN 47
  - VPN-PPTP Server 48
  - VPN-PPTP Client 49
  - VPN-OpenVPN Server 53
  - VPN-OpenVPN Client 56
  - VPN-IPsec 57

Advanced
- Kommandozeileninterface 63
- Systemeinstellung / Update 66
- Logging 67
- Network tracer 68
- User Management 70

Technische Daten 71
mit integr. 4-fach Switch 72
Abmessungen 73
Ländereinstellung Analogrouter 74
Leistungsaufnahme 75
SMS senden 76
Konfiguration GSM, VPN & DynDNS 77

Produktbeschreibung

M2M Industrie Router mit freier Modemwahl, VPN und Firewall

Mit dem M2M-Industrie Router ist eine einfache, sichere und globale Kommunikation zu Ihren Anlagen und Maschinen möglich. Erreicht wird dies durch die integrierte Firewall, VPN-Verbindungen und Tele-Service Dienste. Die kompakte Bauform, das Hutschienen-Gehäuse und die Möglichkeit der internen Modemwahl (Analog, ISDN, GSM/GPRS, UMTS, LTE, DSL) in einem Grundgerät bieten enorme Vorteile.

Der Router verfügt neben der Ethernet auch über eine RS232-Schnittstelle zur Konfiguration (optional mit integriertem 4-fach Switch). Auf Protokollseite unterstützt er SNMP, DHCP, DynDNS, NTP, etc. Konfigurierbare Alarmmeldungen können pper E-Mail verschickt werden. Die digitalen E/A's bieten zusätzlich Kontroll- und Steuermöglichkeiten.

Auf jedem Router befindet sich ein HTML-Webserver mit der kompletten Konfigurationssoftware. Zugriff, Konfiguration und Wartung erfolgt einfach und sicher mit Standard-Webbrowsern. Installation von Drittanbieter-Software nicht nötig.

Bestell-Nummern: ***siehe aktuelle Produktübersicht***

Verbindungsmöglichkeiten des truecon M2M Industrie Routers

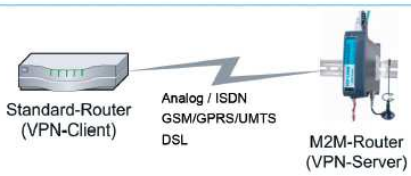
1. Internet Zugriff

- Internet Zugang über Call by Call Provider
- voreingestellte oder frei einstellbare Provider

2. M2M-Router als VPN-Client
Verbindung zu VPN-Server

- VPN- Virtual Private Netzwerk Verbindung übers Internet zu LAN-Netzwerken
- Protokolle: IPSec, PPTP, Open VPN
- DynDNS- feste ROUTER-ALIAS-Namen
- öffentliche IP-Adresse des Routers als E-Mail

3. M2M-Router als VPN-Server
Verbindung zu VPN-Client



- VPN- Virtual Private Netzwerk Verbindung übers Internet zu LAN-Netzwerken
- Protokolle: IPSec, PPTP, Open VPN
- DynDNS- feste ROUTER-ALIAS-Namen
- öffentliche IP-Adresse des Routers als E-Mail

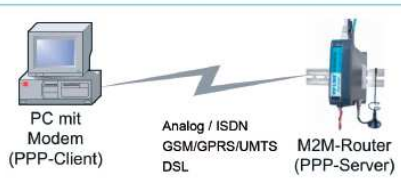
4. M2M-Router zu M2M-Router
VPN-Verbindung Client/Server

- VPN- Virtual Private Netzwerk Verbindung übers Internet zu LAN-Netzwerken
- Protokolle: IPSec, PPTP, Open VPN
- DynDNS- feste ROUTER-ALIAS-Namen
- öffentliche IP-Adresse des Routers als E-Mail

5. PC zu M2M-Router
Software VPN-Client Verbindung

- VPN- Virtual Private Netzwerk Verbindung übers Internet zu LAN-Netzwerken
- Protokolle: IPSec, PPTP, Open VPN
- DynDNS- feste ROUTER-ALIAS-Namen
- öffentliche IP-Adresse des Routers als E-Mail

6. PC zu M2M-Router PPP
PPP-Direktverbindung



- PPP- Point to Point Direktanwahl übers Telefonnetz zur Verbindung mit LAN-Netzwerken
- Call back PPP möglich -Router ruft voreingestellte Nummer direkt (PPP) zurück
- Modems: analog, ISDN und GSM/GPRS/UMTS

Qualifikation des Personals

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal, das mit den geltenden Normen des jeweiligen Einsatzortes vertraut ist. Das Fachpersonal muss diese Dokumentation gelesen und verstanden haben und die Anweisungen befolgen.

Sicherheitsbestimmungen

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz des beschriebenen Produktes alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbaren Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

Auslieferungszustand

Das Produkt wird je nach Anwendung und verwendetes internes Modem in bestimmten Hard- und Firmware-Konfigurationen ausgeliefert. Änderungen der Hard-, oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen sind unzulässig und bewirken den Haftungsausschluss der HY-LINE Systems GmbH. Das Produkt ist nach den derzeit gültigen Regeln der Technik gebaut und betriebssicher und hat das Werk in sicherheitstechnisch einwandfreiem Zustand verlassen.

Um diesen Zustand über die Betriebszeit zu erhalten, sind die Angaben im Handbuch und geltenden Produkt-änderungen (Product Change Notification) und Zertifikate zu beachten und zu befolgen.

Sorgfaltspflicht des Betreibers

Der Betreiber muss sicherstellen, dass

- das Produkt nur bestimmungsgemäß verwendet wird.
- das Produkt nur in einwandfreiem, funktionstüchtigem Zustand betrieben wird.
- nur ausreichend qualifiziertes und autorisiertes Personal das Produkt bedient.
- dieses Personal regelmäßig in allen zutreffenden Fragen von Arbeitssicherheit und Umweltschutz unterwiesen wird,

sowie die Bedienungsanleitung und insbesondere die darin enthaltenen Sicherheitshinweise kennt.

Der Betreiber muss grundsätzlich die in seinem Land geltenden nationalen Vorschriften bezüglich Betrieb, Funktionsprüfung, Reparatur und Wartung von elektronischen Geräten beachten.

Bestimmungsgemäße Verwendung

Das Produkt darf nur innerhalb der spezifizierten Angaben aus diesem Dokument und Dokumenten, auf die verwiesen wird, verwendet werden. Das Produkt darf nicht zu den folgenden Zwecken und unter diesen Bedingungen verwendet oder betrieben werden: Steuerung oder Schaltung von Maschinen und Anlagen, die nicht der Richtlinie 2006/42/EG sowie der Richtlinie 2004/108/EWG (EMV - Richtlinie) entsprechen.

Es wird empfohlen, folgendes Netzteil mit dem HY-LINE Router zu verwenden, da alle EMV-Tests mit diesem Netzteil durchgeführt wurden:

- HAP-RUx - UMTS Router Versionen: Netzteil MinWa MC120D050 12W mit Ferrit Würth 74270077

- alle anderen Router Versionen: Netzteil PHI-CON: PS18A120

Lesen Sie vor Installation und Inbetriebnahme diese Dokumentation vollständig durch. Falsches Handhaben des Produktes kann zu Personen- oder Sachschäden führen. Halten Sie die technischen Daten und die Angaben zu den Anschlussbedingungen unbedingt ein.

Lizenzen

Die in diesem Produkt inbegriffene Software enthält urheberrechtlich geschützte Software, die unter der GPL oder anderer kostenloser Lizenzen lizenziert ist. Sie können den vollständigen entsprechenden Source-Code von uns zum Selbstkostenpreis für einen Zeitraum von drei Jahren seit der letzten Auslieferung dieses Produkts anfordern. Bitte wenden Sie sich mit dem Betreff: 'Source-Code für truecon Router' an: HY-LINE Systems GmbH, Inselkammerstr. 10, 82008 Unterhaching, Deutschland. E-Mail: systems@hy-line.de Dieses Angebot gilt für jeden nach Erhalt dieser Mitteilung.

Technische Grenzwerte

Das Produkt ist ausschließlich für die Verwendung innerhalb der in den Datenblättern angegebenen technischen Grenzwerte bestimmt. Folgende Grenzwerte sind einzuhalten:

- Die angegebene Umgebungstemperatur darf nicht unter- bzw. überschritten werden.
- Der angegebene Versorgungsspannung darf nicht unter- bzw. überschritten werden.
- Die maximale Luftfeuchtigkeit darf nicht überschritten werden, sowie Kondensatbildung ist zu vermeiden.
- Die maximale Schaltspannung, sowie maximale Schaltstrombelastung darf nicht überschritten werden.
- Die maximale Eingangsspannung, sowie der maximale Eingangsstrom darf nicht überschritten werden.

Gewährleistungsbestimmung

Das Produkt ist wartungsfrei. Bei Öffnen des Gehäuses erlischt jegliche Gewährleistung. Reparaturen dürfen nur durch autorisiertes Fachpersonal durchgeführt werden. Bei unbefugten Eingriffen erlischt jede Gewährleistung.

Eine nicht bestimmungsgemäße Verwendung, ein Nichtbeachten dieser Dokumentation, der Einsatz von unzureichend qualifiziertem Personal sowie eigenmächtige Veränderungen schließen die Haftung des Herstellers für daraus resultierende Schäden aus.

Hinweise zu Transport und Lagerung

Bitte Umweltbedingungen für Lagerung beachten: unzulässige Beanspruchungen wie mechanische Belastung, Temperatur, Feuchtigkeit, aggressive Atmosphäre vermeiden.

Das Produkt ist so zu verpacken, dass es vor Erschütterungen beim Transport und bei der Lagerung geschützt ist.

Bitte das Produkt vor Installation auf mögliche Beschädigungen überprüfen, die durch unsachgemäßen Transport oder unsachgemäße Lagerung entstanden sein könnten.

Sicherheitshinweise zur elektrischen Installation

Die Montage muss gemäß Dokumentation und mit geeigneten Werkzeugen erfolgen. Die Montage des Produktes darf nur im spannungsfreien Zustand erfolgen. Bei Verdrahtungsarbeiten ist der Schaltschrank gegen Wiedereinschalten zu sichern. Die nationalen geltenden Unfallverhütungsvorschriften sind einzuhalten. Die elektrische Installation ist gemäß nationalen Vorschriften (Leiterfarben, -Querschnitte, Absicherungen, Schutzleiteranschluss, usw.) auszuführen.

Elektrische Arbeiten dürfen nur von autorisiertem Fachpersonal vorgenommen werden. Die Hinweise zum elektrischen Anschluss in der Dokumentation beachten, ansonsten kann die elektrische Schutzart beeinträchtigt werden.

Entsorgung

Das Produkt in seinem Lieferumfang besteht aus verschiedenen Materialien:

Die einzelnen Komponenten müssen fachgerecht entsorgt werden. Alle Bestandteile des Lieferumfanges können zu HY-LINE Systems zur fachgerechten Entsorgung zurückgesendet werden. Die Transportkosten gehen zu Lasten des Absenders.

Lieferumfang

Der Lieferumfang für den HY-LINE Router umfasst die im Folgenden aufgeführten Zubehörteile. Bitte kontrollieren Sie, ob alle angegebenen Zubehörteile in Ihrem Karton enthalten sind. Sollte ein Teil fehlen oder beschädigt sein, so wenden Sie sich bitte an Ihren Distributor.

1 HY-LINE Router (verschiedene Grundtypen)

1 Quick Installation Guide

1 GSM-Antenne mit Magnetfuß

Weiterführende Dokumente für den HY-LINE Router sind verfügbar unter: www.hy-line.de/router

HY-LINE Router Varianten

- **Analog: HAP-RA**
- **mit integr. 4-fach Switch: HAP-RAS**

- **ISDN: HAP-Ri**
- **mit integr. 4-fach Switch: HAP-RiS**

- **UMTS : HAP-RU**
- **mit integr. 4-fach Switch: HAP-RUS**

- **DSL : HAP-RDS / HAP-RDSH**
- **mit integr. 4-fach Switch**

- **HAP-R – ohne integr. Modem**
- **mit integr. 4-fach Switch: HAP-RS**

- **LTE : HAP-RL**
- **mit integr. 4-fach Switch: HAP-RLS**

- **alle Varianten auch mit integr. 8-fach Switch verfügbar!**

Anzeigen- und Bedienelemente

HAP-R
HAP-RI
HAP-RA
HAP-RG
HAP-RU
HAP-RL

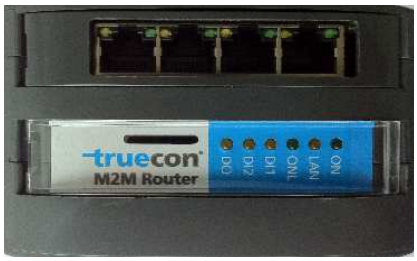
HAP-RS
HAP-RIS
HAP-RAS
HAP-RGS
HAP-RUS
HAP-RLS

integr. 4-fach Switch

HAP-RDS

integr. 4-fach Switch

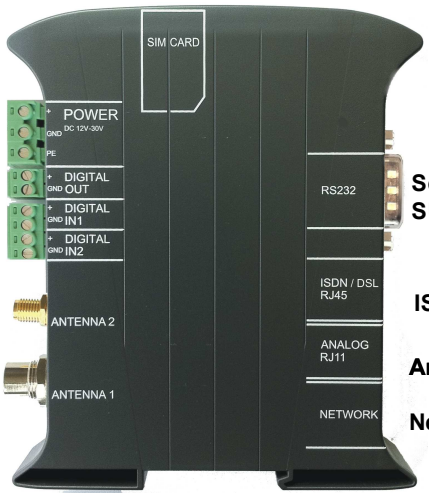
SIM-Kartenschlitz



Power (10-30VDC) Digital I/Os (Schraubklemmen, abziehbar)

Antenne 2 - SMA: GSM/UMTS (optional)

Antenne 1 - FME: GSM/UMTS



Seriell RS232– SUB-D 9polig

ISDN/DSL RJ45

Analog RJ11

Netzwerk RJ45

Unterseite: Hutschienenbefestigung

-> Aus EMV-technischer Sicht empfiehlt es sich, die Antennen-Buchsen 1 und 2 mit PE (Potential Erde) am Versorgungsstecker des Routers zu verbinden. Dieses PE-Signal dann auf Schaltschrankmasse auflegen.

Buchsen- und Steckerbelegung:

Wichtig: die einzelne Netzwerkbuchse RJ45 auf der Seite des Routers ist bei der Router Version mit integriertem Switch nicht belegt und darf nicht verwendet werden. Diese ist im Auslieferzustand mit einem Blindstopfen versiegelt. Dieser darf nicht entfernt werden.

Router Version	Buchse – ISDN/DSL	Buchse – Analog
UMTS/GPRS - HAP-RU/RUS	nicht belegt	nicht belegt
DSL - HAP-RDS	belegt (Pin 4/5 – DSL A/B)	nicht belegt
Analog - HAP-RA/RAS	nicht belegt	belegt (Pin 3/4 – TX/RX)
ISDN - HAP-RI/RIS	belegt (Pin 3/4/5/6 – TX+/TX-/RX+/RX-)	nicht belegt
ohne internes Modem - HAP-R/RS	nicht belegt	nicht belegt

Inbetriebnahme - *Schnellanleitung:*

Download Router Handbuch: www.hy-line.de/router

Zugang zum Router über WEB-Browser (mit Default-IP-Adresse im Auslieferzustand):
http://192.168.101.222/ oder https://192.168.101.222/

Administratorzugang:
login: *manager* **passwort**: changemetoo (Passwort kann über User-Management geändert werden)

Beobachterzugang:
login: user **passwort**: changeme (Passwort kann über User-Management geändert werden)

Zugang zum Router über SSH-Secure Shell (TCP/IP):

login: *root* **passwort:** *changemetoo*
Einstellung SSH (TCP/IP): Host-Name oder IP-Addresse: *Router-IP* Port: *22*

Hinweis: Zur ersten Initialisierung des SSH-Keys muss der Router für ca. 10 Minuten eingeschaltet sein. Danach ist der Router per SSH erreichbar!

Zugang zum Router über serielle Konsole (Nullmodemkabel):

login: *root* **passwort:** *changemetoo*
Einstellung serielle Schnittstelle: 38.400 bps // 8 Datenbits // keine Parität // 1 Stoppbit // keine Flussteuerung

IP-Adresse ändern über SSH oder serielle Konsole:
1) Einloggen auf SSH oder seriell wie oben beschrieben
2) Befehle ausführen wie folgt:
    1. ip address xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx device eth0
    2. commit ch
    3. write disk

Installation der SIM-Karte bei GSM/GPRS/UMTS-Router nur im stromlosen Zustand:
Chipseite (gold) der SIM-Karte zeigt zur Router-Gehäuseseite ohne Aufdruck, SIM-Karte muß einrasten

LED- Signalisierung

LED ON	Leuchtet sobald das Gerät mit Spannung versorgt wird
LED LAN	Leuchtet: LAN-Kabel eingesteckt mit aktivem Netzwerk, Blinkt bei LAN Zugriff
LED ONL	Leuchtet: Internetverbindung oder PPP-Einwahl aktiv
LED DI1	Leuchtet sobald an Digital IN1 Spannung anliegt oder kurzgeschlossen als potentialfr. Kontakt
LED DI2	Leuchtet sobald an Digital IN2 Spannung anliegt oder kurzgeschlossen als potentialfr. Kontakt
LED DO	Leuchtet: Digital Out über Webseite geschaltet oder Mapping von DigIN1 oder DigIN2
LED DSL Sync	Blinkt: DSL Verbindung wird aufgebaut Leuchtet: DSL Synchronisierung erfolgreich -> die DSL Sync Lampe (blau) befindet sich im Inneren des Routers. Diese sieht man von Außen durch die Lüftungsschlitze auf der Seite des Spannunsgversorgungsstecker

Inbetriebnahme - *Schnellanleitung:*

Hinweis: jede Einstellung muß mit der SAVE-Schalfläche auf der jeweiligen Seite bestätigt werden, am Ende der Konfiguration muß der Router neu gebootet werden

1. Montage: Um eine ausreichende Belüftung des Routers zu gewährleisten, darf dieser nur auf der Hutschiene montiert betrieben werden. Die Spannunsgversorgungsanschlüsse zeigen nach unten.
2. Router stromlos schalten, bei GSM/UMTS Router die SIM-Karte in Router einstecken, Router einschalten
3. im Menü \Base Settings\Network\ die IP Einstellungen auf Ihre IT-Infrastruktur anpassen
4. im Menü \Connectivity Settings\Modem Settings\ die PIN der SIM Karte eintragen und PIN enablen (falls SIM Karte durch Pin geschützt ist)
5. im Menü \Connectivity Settings\Internet Settings\ den gewünschten Internet Service einstellen, mit SET bestätigen; APN (bei GSM/GPRS/UMTS-Betrieb), Benutzername und Passwort einstellen. Falls gewünscht, das DynDNS Protokoll (unter IP reporting mode) aktivieren.
6. im Menü\Services\DHCP\ die IP-Range auf Ihre Infrastruktur anpassen (nur notwendig bei Verwendung des Router als DHCP Server), ansonsten DHCP Server deaktivieren
7. DynDNS Einstellung: im Menü \Services\DynDNS\ hier die Daten zum DynDNS eintragen (Benutzername und Passwort zum Einloggen am DynDNS Server, ALIAS Name für den M2M Router)

Einstellungen der Geräte im lokalen Router Netz:
In diesen Geräten muß die IP-Adresse des M2M Routers als Gateway eingetragen sein.

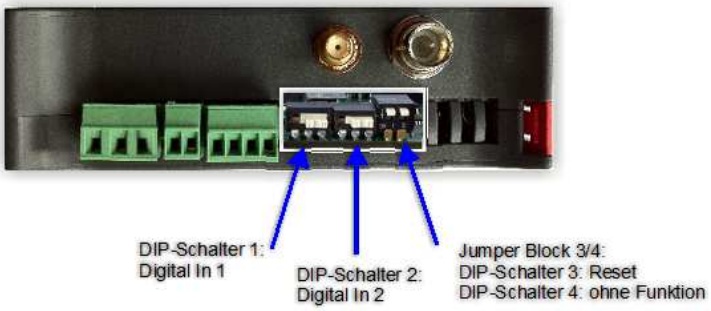
Testen einer bestehenden Internetverbindung:
Die Internet Verbindungstest Schaltfläche auf der HOME Seite des Routers drücken. Es öffnet sich ein weiteres Fenster, in dem das ping-Ergebniss angezeigt wird. Die Ping-Zieladresse ist im Menü \Services\InetWD einstellbar.

Softwarereset: Rücksetzen aller Einstellungen auf Auslieferzustand

1. Trennen Sie den Router von der Spannungsversorgung
2. Auf der Router Seite mit dem Spannungsanschluss muß hinter den Lüftungsschlitzen der Jumper 3 auf ON (zur Router Grundplatine hin) geschaltet werden (siehe Bild unten, Jumper 3 ist der linke Jumper vom Jumper Block 3/4)
3. Router nun Einschalten und ca. 2 Minuten warten. Der Reset Vorgang ist abgeschlossen, wenn die LEDs zyklisch an und ausgehen (Lauflicht)
4. Trennen Sie den Router von der Spannungsversorgung
5. Setzen Sie Jumper 3 auf die OFF Position (weg von der Router Grundplatine) zurück
6. Starten Sie den Router neu, alle Einstellungen wurden zurückgesetzt

Die Position der Jumper (hinter den Lüftungsschlitzen) im Bild zeigt die Konfiguration (Auslieferungszustand) von DigEin1 und DigEin2 als potentialfreie Eingänge (siehe Kapitel I/O-Settings Input / Output)

Die Jumper nur im ausgeschalteten Zustand des Routers setzen. Das Gehäuse dafür nicht öffnen!



Konfiguration - *Home:*

Die Startseite enthält eine Übersicht über:

- Router Firmware Version und Seriennummer,
- System uptime: Laufzeit des Routers
- Digital I/O: Status der digitalen Eingänge und des Ausgangs

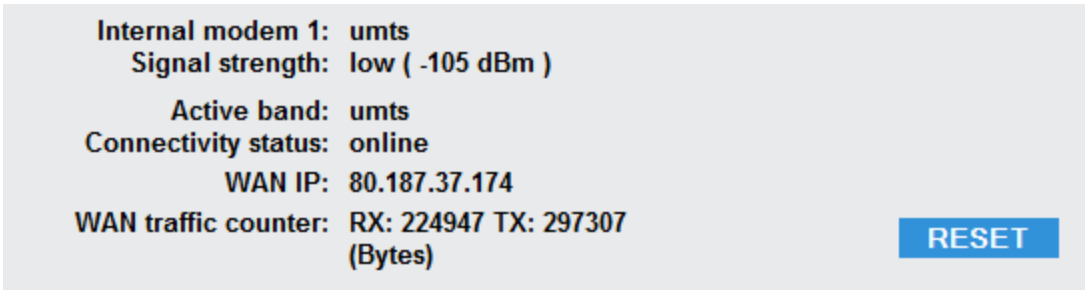
Konfiguration - *Home:*

- Internes Modem 1: analog, isdn, gsm, umts, lte, dsl, none (entspricht ohne Modem)
- Signalstärke:

Error	kein Signal vorhanden oder SIM Karte mit PIN gesperrt
Bad	-113 ... -112 dBm
Low	-111 ... – 90 dBm
Good	- 89 ... – 56 dBm
Very good	> -55 dBm

- Aktives Band:
  lte
  umts/WCDMA2100
  gsm1800 (gprs-1800 MHz Band)
  gsm900 (gprs-900 MHz Band)
  no Service (keine SIM-Karte oder kein Antennensignal)

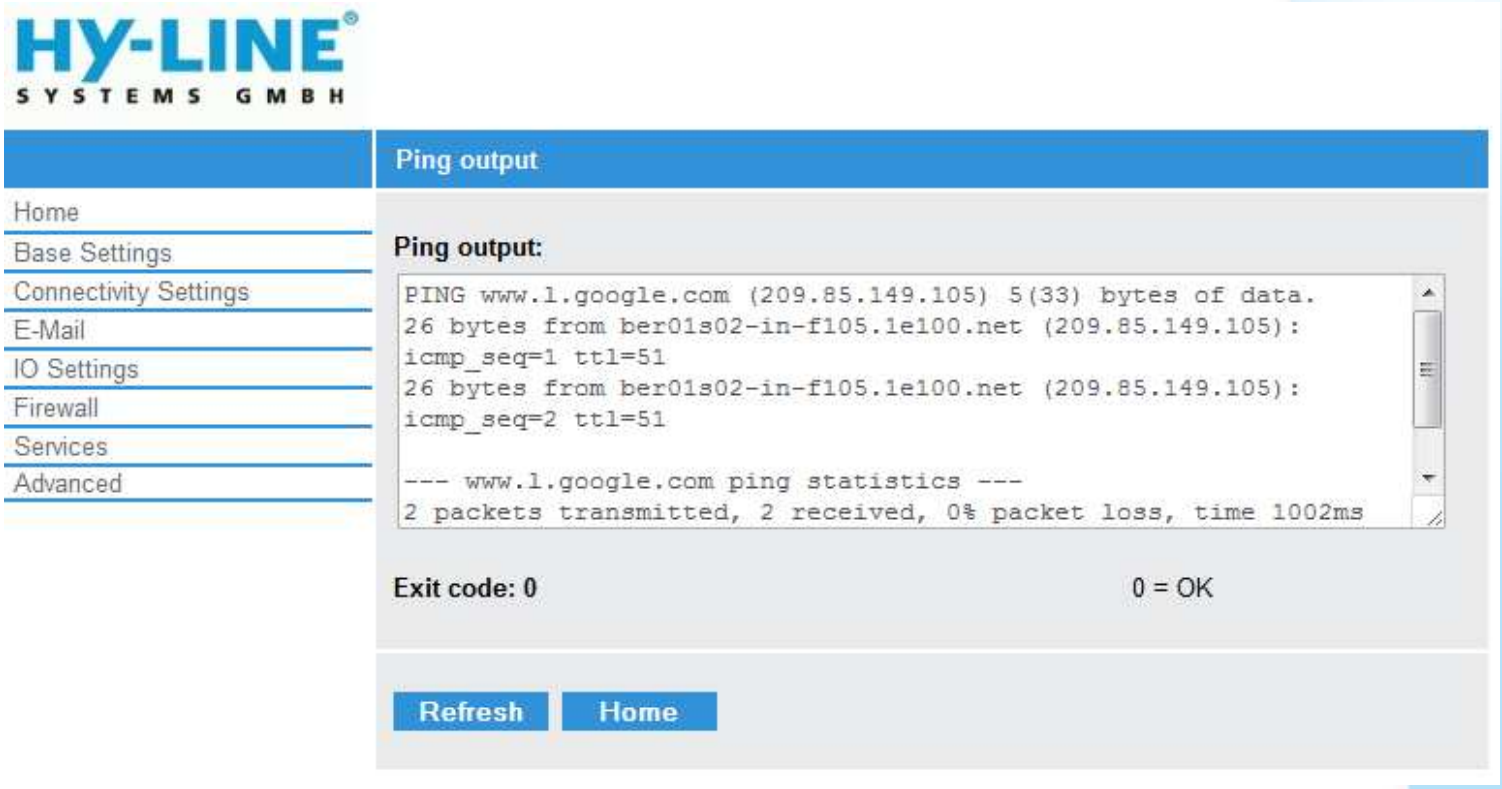
- Connectivity status: Status der Internetverbindung: bei bestehender Online Verbindung zeigt der Router seine momentane öffentliche IP-Adresse (vom Provider zugewiesen) an:


Internal modem 1: umts
Signal strength: low (-105 dBm)
Active band: umts
Connectivity status: online
WAN IP: 80.187.37.174
WAN traffic counter: RX: 224947 TX: 297307 (Bytes)
RESET

- **WAN Traffic Counter:** Datenvolumenzähler Internet und PPP-Traffic, max. 2.147.483.648 Bytes
- **Reset-Taste:** Rückstellen des Datenvolumenzählers

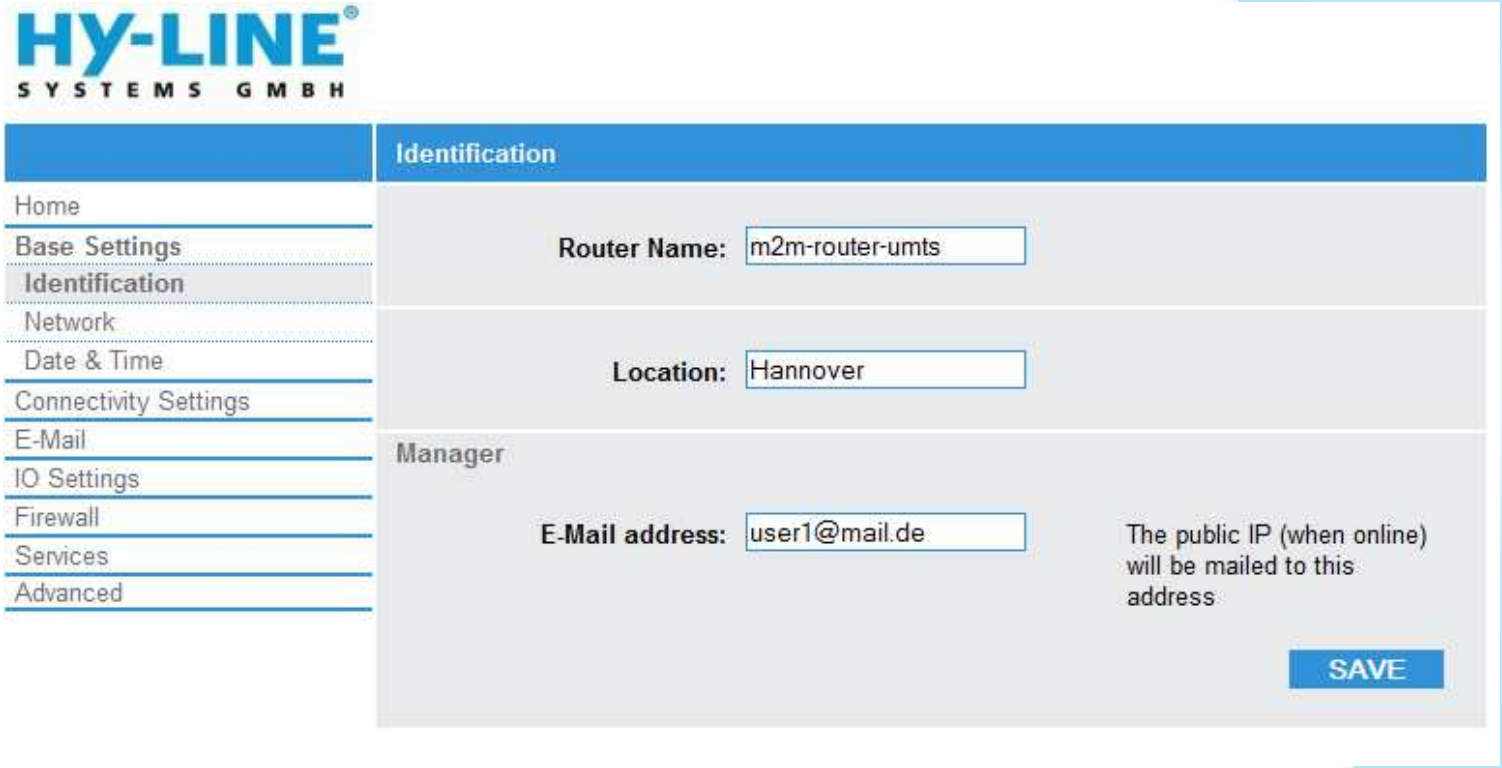
Konfiguration - *Home:*

- **DNS Servers:** verwendete DNS Server
- **Default Gateway:** aktive Gateway (siehe auch Konfiguration Base settings – LAN 2)
- **Internet Connectivity:** Mit dem Test Button wird ein ping über das Default Gateway abgeschickt. Falls der Router ein internes Modem hat und nicht im Internet eingewählt ist, erfolgt die Interneteinwahl umgehend. Der Zieladresse des Pings kann unter ..\Services\InetWD geändert werden.



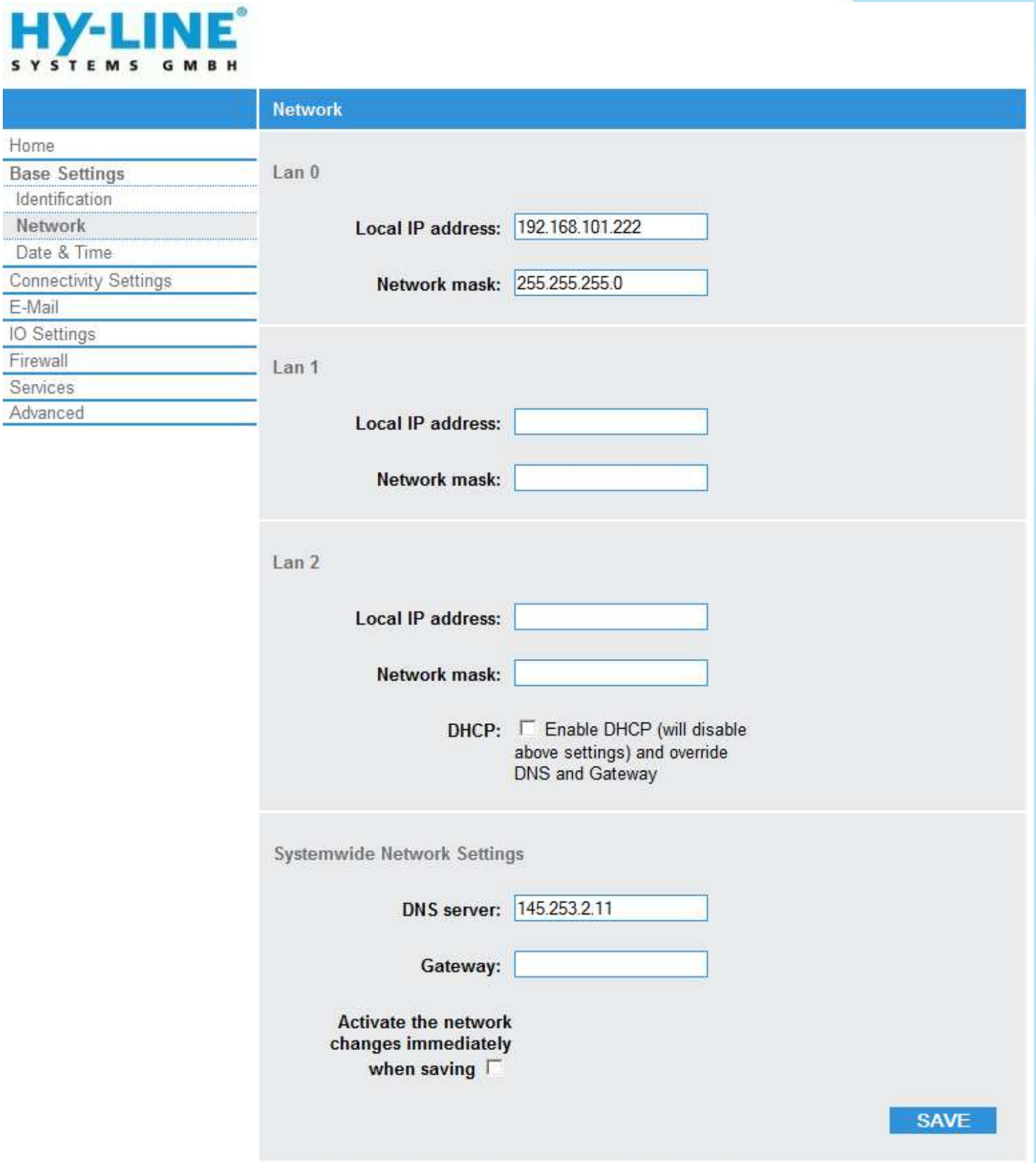
- **Refresh-Taste:** wiederholt den ping Befehl
- **Home-Taste:** zurück zum Router Home Bildschirm
- **Reboot-Taste:** Router (Software) Neustart
- **Redundanz Status:** Aktiviert / Zustand

Base Settings - Identification:



- **Router Name:** Name des Routers mit max. 35 Zeichen , wird in der E-Mail angezeigt
- **Location:** Ortsangabe des Routers
- **Manager:** E-Mail Adresse des System Managers, Empfänger der öffentlichen IP-Adresse per E-Mail sobald der M2M Router ins Internet eingewählt ist

Base Settings - Network:



Base Settings - Network:

Die LAN-Settings konfigurieren die Schnittstellen eth0, eth0:1 und eth0:2. Die :x sind "virtuelle" Interfaces, die physikalisch auf eth0 gemappt werden. Dadurch werden mehrere Adressen auf einem Interface abgebildet.

- **LAN 0 – LAN 2:**

Local IP-Adresse / Network mask: Parameter für die Subnetze (Multirouting)

- **Systemwide Network Settings:**

DNS Server: Netzwerk DNS Server Adresse (Default ist ein öffentlicher DNS Server)

Gateway: Netzwerk Gateway Adresse

Activate network changes: aktivieren, um Einstellungen sofort nach SAVE zu übernehmen

- **Konfiguration Multi-LAN:**

- DHCP ist auf ein virtuelles Interface eingeschränkt: LAN2 (eth0:2)

- Der DHCP Client übernimmt neben der IP Adresse und Netzwerkmaske auch den DNS Server und das Defaultgateway.

- Die Einstellungen auf der Netzwerkseite für DNS und Gateway werden vom DHCP Client überschrieben, jedoch nicht in den Eingabefeldern ausgelesen und angezeigt.

- Folgende, vom DHCP bezogene Informationen, werden auf der HOME Seite angezeigt:

* DNS Adressen * DHCP Address / Netzmaske * Defaultroute

- **Externes Gateway zur Datenübertragung (Router: kein internes Modem oder nicht aktiv)**

- Service: Internet-Dial-Up deaktivieren im Service Menü
- Wird der HY-LINE Router ‚hinter' einem Gateway betrieben, müssen die Netzwerkeinstellungen wie folgt vorgenommen werden:

DHCP-Server inaktiv im ext. Gateway Subnetz:

LAN 0: Netzwerk/Subnetz auf der der Gateway Seite
LAN 2: Netzwerk/Subnetz des HY-LINE Routers
Gateway (systemwide): Netzwerk/Subnetz auf der der Gateway Seite

DHCP-Server aktiv im ext. Gateway Subnetz:

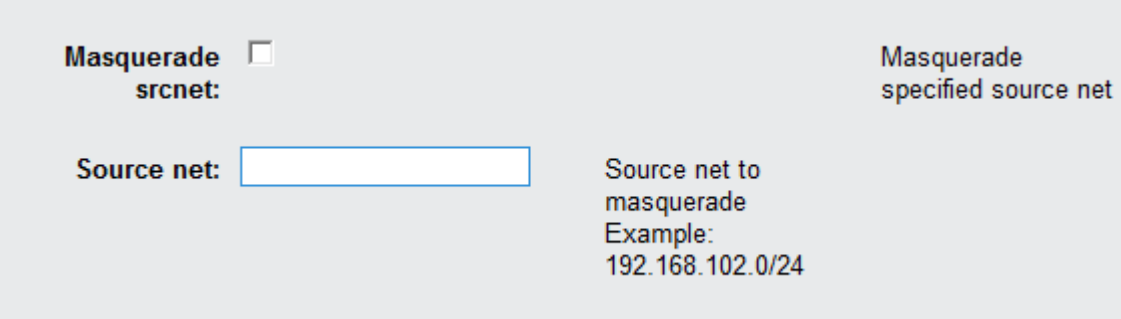
LAN 0: Netzwerk/Subnetz des HY-LINE Routers
LAN 2: Netzwerk/Subnetz auf der der Gateway Seite (DHCP aktivieren)
Gateway (systemwide): Netzwerk/Subnetz auf der der Gateway Seite (wird autom. vergeben)

Base Settings - Network:

- **Fortsetzung: externes Gateway zur Datenübertragung**

Ausgehende Verbindungen (HY-LINE Router LAN -> externe Gateway) :

Service Menü Firewall:



- **Masquerade srcnet:** Aktivieren: erlaubt ausgehende TCP-Pakete über ein Standard Gateway (keine Modemgateway)

- **Source net:** Netzmaske/IP-Bereich des zu ausgehenden Traffic
  Beispiel: 172.1.2.0/8 - 255.0.0.0
  172.1.0.0/16 - 255.255.0.0
  172.0.0.0/24 - 255.255.255.0

Darstellung Ipv4 Netzadressen und Netzmasken

(Quelle: Wikipedia: http://de.wikipedia.org/wiki/Netzmaske)

Bits

Eine Netzmaske ist genau so lang wie eine IPv4-Adresse, also 32 Bit. Alle Bits des Netzwerkteils sind auf 1 gesetzt, alle Bits des Geräteteils haben den Wert 0. Der Netzwerkteil einer IPv4-Adresse ergibt sich aus ihrer bitweisen logischen AND-Verknüpfung mit der Netzmaske. Nach der bitweisen Negation der Netzmaske wird der Geräteteil ebenso abgetrennt.

Beispiel

	IPv4-Adresse	11000000 10101000 00000001 10000001
UND	Netzmaske	11111111 11111111 11111111 00000000
=	Netzwerkteil	11000000 10101000 00000001 00000000

	IPv4-Adresse	11000000 10101000 00000001 10000001
UND	NOT Netzmaske	00000000 00000000 00000000 11111111
=	Geräteteil	00000000 00000000 00000000 10000001

Fortsetz.

Darstellung Ipv4 Netzadressen und Netzmasken

(Quelle: Wikipedia: http://de.wikipedia.org/wiki/Netzmaske)

Bei einer solchen Netzmaske mit 24 gesetzten Bits verbleiben 8 Bits und damit 28=256 Adressen für Geräteteile. Man spricht von einem 24-Bit-Netz. Weil die kleinste Adresse (alle Bits im Geräteteil sind null) das Netz selbst beschreibt und die größte Adresse (alle Bits im Geräteteil sind eins) für den Broadcast reserviert ist, zählen sie nicht zu den Adressen, die an Geräte verteilt werden. Es stehen also 254 Adressen für Geräte zur Verfügung.

Die Notation von Netzmasken wie IPv4-Adressen erfolgt in der Regel im Dezimalsystem. Dann lautet die IP-Adresse des obigen Beispiels 192.168.1.129 und die Netzmaske 255.255.255.0 oder kurz /24. Somit ist der Netzwerkteil 192.168.1 und der Geräteteil 129. Das IP-Netz kann man auch als 192.168.1.0/24 beschreiben.

Während die CIDR-Notation /24 die Anzahl der in der Netzmaske gesetzten Bits angibt, wird die Netzmaske bei der dotted decimal notation in vier Oktette zerlegt, die durch Dezimalzahlen dargestellt werden. Die Dezimalzahl 255 hat den gleichen Wert wie die Dualzahl 11111111, die 8 gesetzten Bits entspricht. So ergeben sich im Beispiel 8+8+8+0=24 gesetzte Bits. Eine Übersicht über alle IPv4 Netzmasken größer als /8 in verschiedenen Notationen befindet sich im Artikel CIDR.

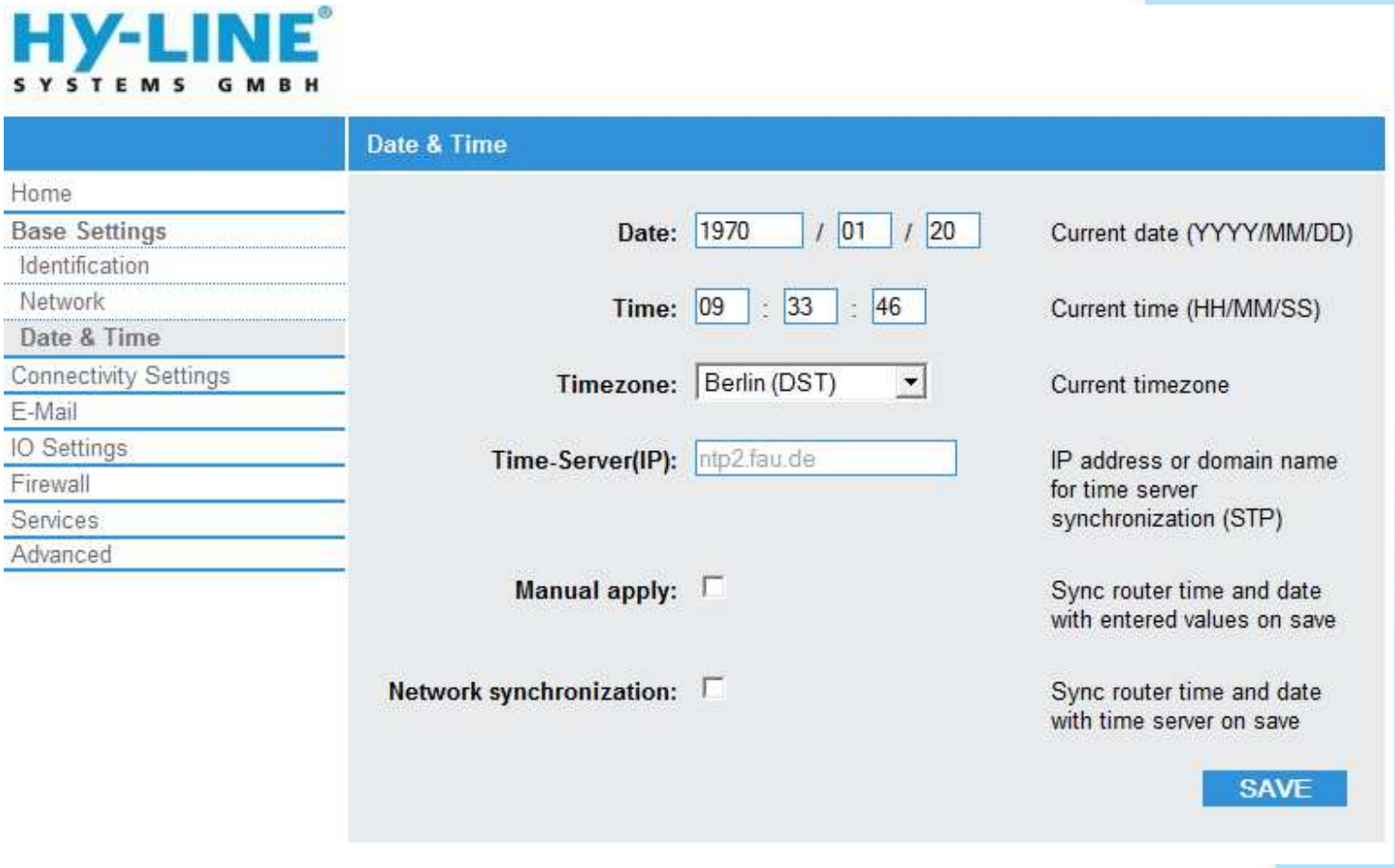
Beispiel 1:

Untersucht werden soll die IP-Adresse 192.168.1.188/27, in anderer Schreibweise 192.168.1.188/255.255.255.224. Die Netzwerkmaske ist eine 27-Bit-Maske. Zuerst soll die Frage geklärt werden, wie viele IP-Adressen zu einem 27-Bit-Netz gehören. Antwort: Eine IPv4-Adresse besteht aus 32 Bits. 32 minus 27 ist 5. Die 27-Bit-Maske lässt also 2 hoch 5 Adressen zur freien Verfügung, d. h. 32. Zu einem 27-Bit-Netz gehören somit 32 Adressen. Nun soll die Frage geklärt werden, wie das Netz heißt, zu dem die Adresse gehört. Antwort: Die kleinste Adresse aus dem vorbestimmten Umfang gibt dem Netz seinen Namen. Man findet sie, indem man von 188 ausgehend die nächste kleinere Zahl sucht, die durch 32 teilbar ist. Es ergibt sich 160. Das Netz heißt also 192.168.1.160/27. Zu ihm gehören die 32 Adressen von 192.168.1.160 bis einschließlich 192.168.1.191. Die Adresse 192.168.1.160 bezeichnet das Netz selbst, 192.168.1.191 ist die Broadcast-Adresse. Für Geräte nutzbar bleiben die 30 IP-Adressen von 192.168.1.161 bis einschließlich 192.168.1.190.

Beispiel 2:

172.16.0.0/16 und 172.16.0.0/24 unterscheiden sich dadurch, dass das erste Netz die IP-Adressen 172.16.0.1 bis 172.16.255.254 umfasst, während das zweite nur den Bereich 172.16.0.1 bis 172.16.0.254 beinhaltet.

Base Settings - Date & Time:

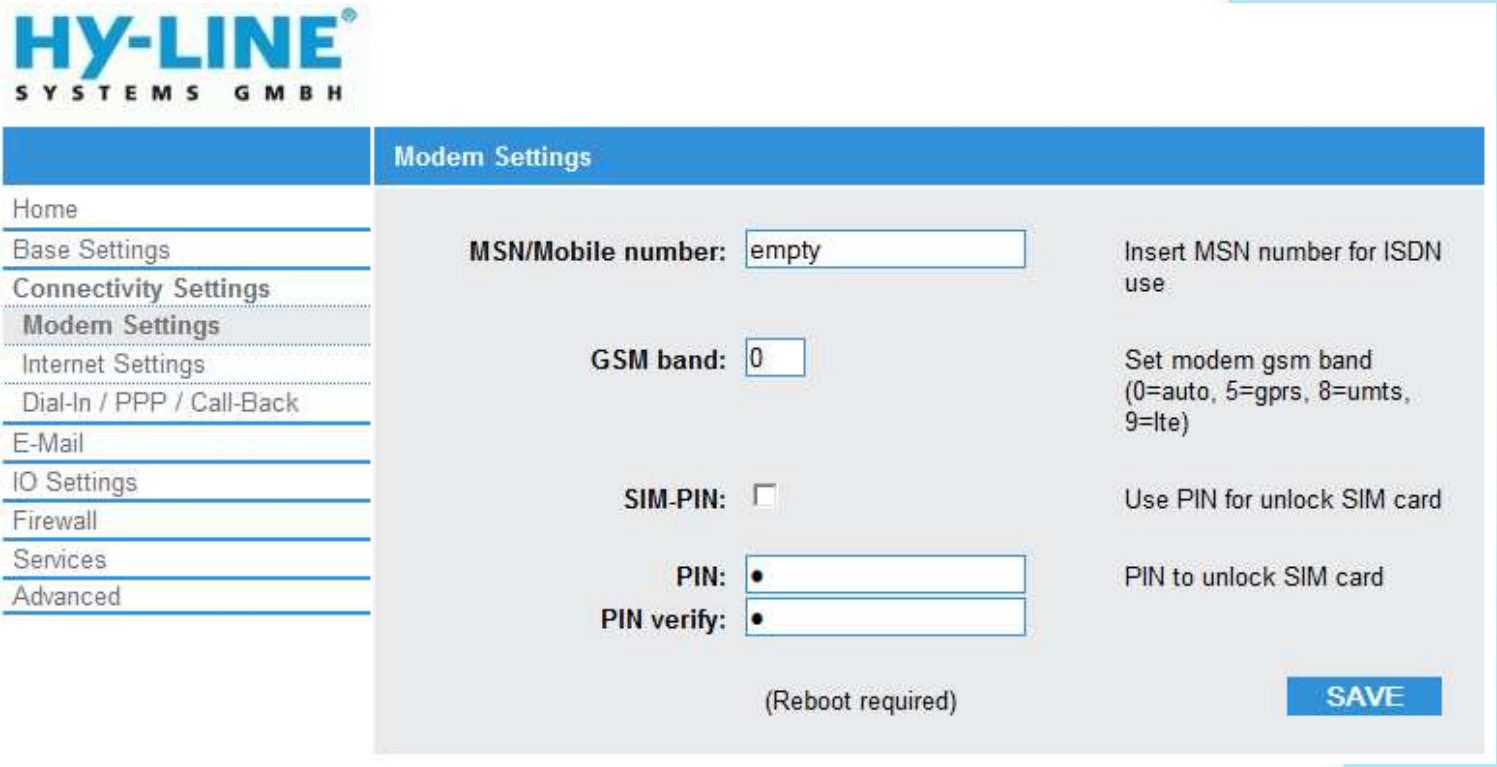


- **Date, Time:** Datum und Uhrzeit des Router
- **Timezone:** Zeitzone in der sich der Router befindet :

  Berlin (DST): in dieser Einstellung wird automatisch die Sommer- und Winterzeit umgestellt (Zeitzone GMT+1)

- **Time-Server:** Zeitserver, Standard TU Braunschweig: ptbtime1.ptb.de
- **Manual apply:** manuelles Einstellen der Uhrzeit & Datum
- **Network sync.:** Zeit & Datum wird per Internet synchronisiert nach Drücken auf SAVE, im Bedarfsfall wählt sich der Router ins Internet ein

Connectivity Settings – Modem Settings:



- **MSN/Mobile number:**
  MSN des ISDN-Anschlusses. Die MSN (Multiple Subscriber Number) ist entweder die Rufnummer ohne Vorwahl oder nur die Durchwahl am vorhandenen Telefonanschluß. Dies ist abhängig von der Konfiguration Ihres Telefonanschlusses. Alternativ kann hier bei Analog/UMTS/DSL Routern eine Rufnummer als statische Anzeige eingetragen werden (ohne Funktion).

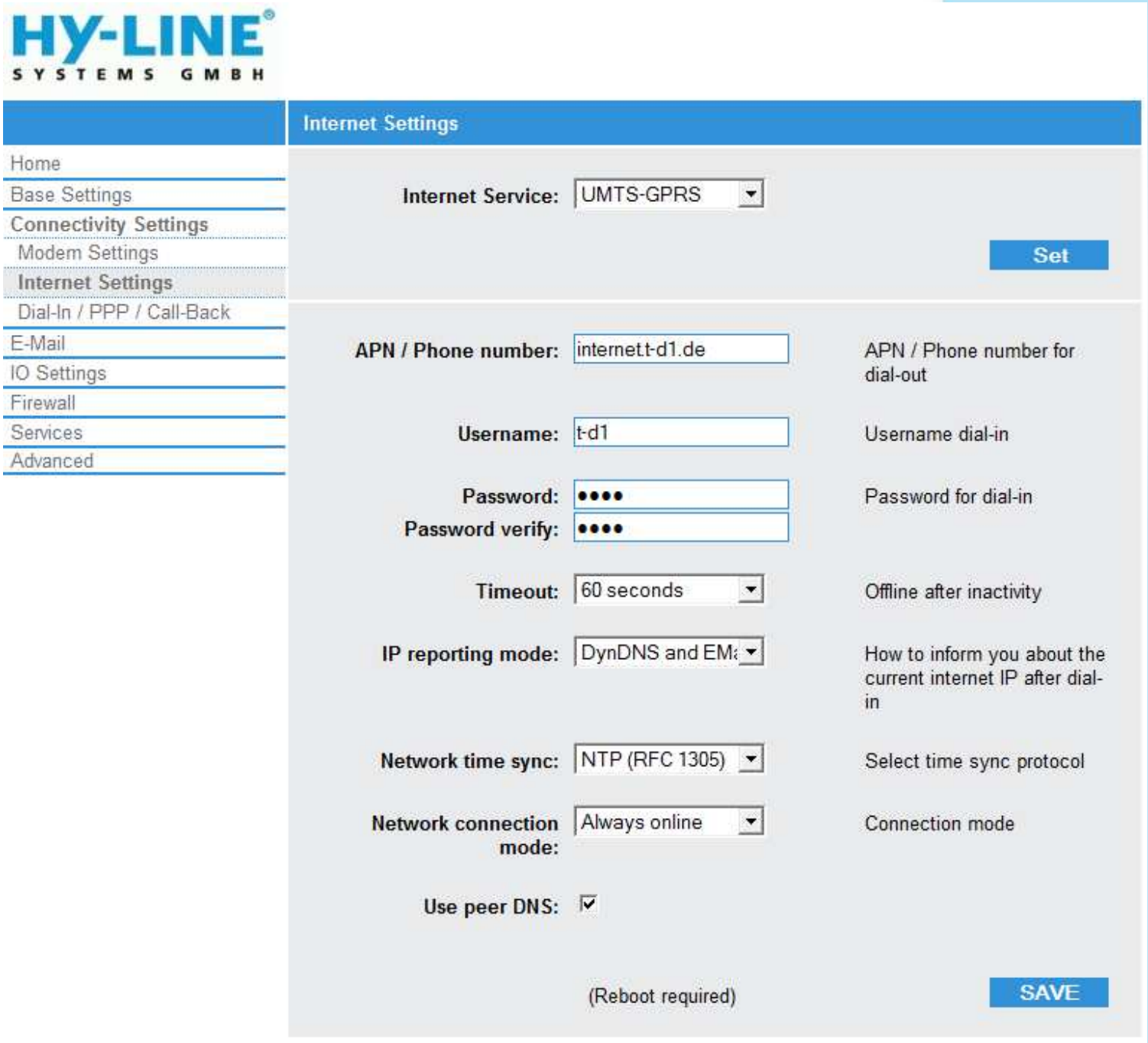
- **GSM band:** Manuelle GSM Band Auswahl. Optionen: 0=auto; 5=gprs; 8=umts; 9=lte

- **SIM-PIN:** Der Router setzt beim Starten die PIN Nummer der SIM-Karte - Darf bei Analog und ISDN Modembetrieb nicht aktiviert sein!

- **PIN:** Pin-Nummer der SIM-Karte

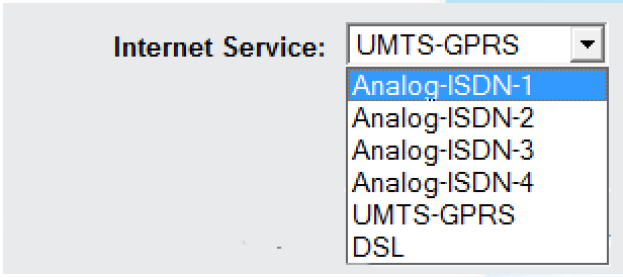
- **PIN verify:** Bestätigung der Pin-Nummer

Connectivity Settings – Internet Settings:



Connectivity Settings – Internet Settings:

- **Internet Service:** Auswahl des Internet Service



  - UMTS-GPRS: Voreinstellung TELEKOM
  - Analog-ISDN 1: Voreinstellung Arcor
  - Analog-ISDN 2: Voreinstellung Freenet
  - Analog-ISDN 3: Voreinstellung T-Online
  - Analog-ISDN 4: Voreinstellung Schweiz
  - DSL

- **PPPoE - externes Modem zur Datenübertragung (Router: kein internes Modem oder nicht aktiv)**

- PPPoE aktivieren: Connectivity Settings\Internet Settings\Internet Service: DSL
- Externes Modem an beliebigen Ethernet-Port am HY-LINE Router verbinden
- PPPoE mit externen Modem funktioniert nicht in der HY-LINE Router Version mit internen DSL-Modem

- **APN / Phone number:** APN bei GPRS/UMTS-Betrieb
  Telefonnummer des Internet Providers bei Call-by-Call, Wählpausen mit Kommatas einfügen (2 Sekunden pro Komma, z.B. 0,,Telefonnummer)

- **Username:** Benutzername für den Internet
- **Password:** Passwort für den Internet Zugang

-> Username und Passwort Felder dürfen nicht leer bleiben. Verlangt der ISP keine Daten, einfach unverändert lassen.

- **Password verify:** Passwort Bestätigung Internet Zugang

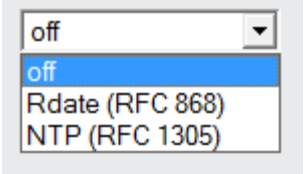
- **Timeout:** Zeit bis zum automatischen Trennen der Telefonverbindung bei Inaktivität. Im Modus ‚Persistent' keine Funktion.

- **IP reporting mode:** nach Internet Einwahl: DynDNS aktiviert und/oder öffentliche IP-Adresse des Routers per E-Mail

- **Network time sync (siehe auch Einstellungen im Service Menü unter NTPd):**

Zeitsynchronisation:

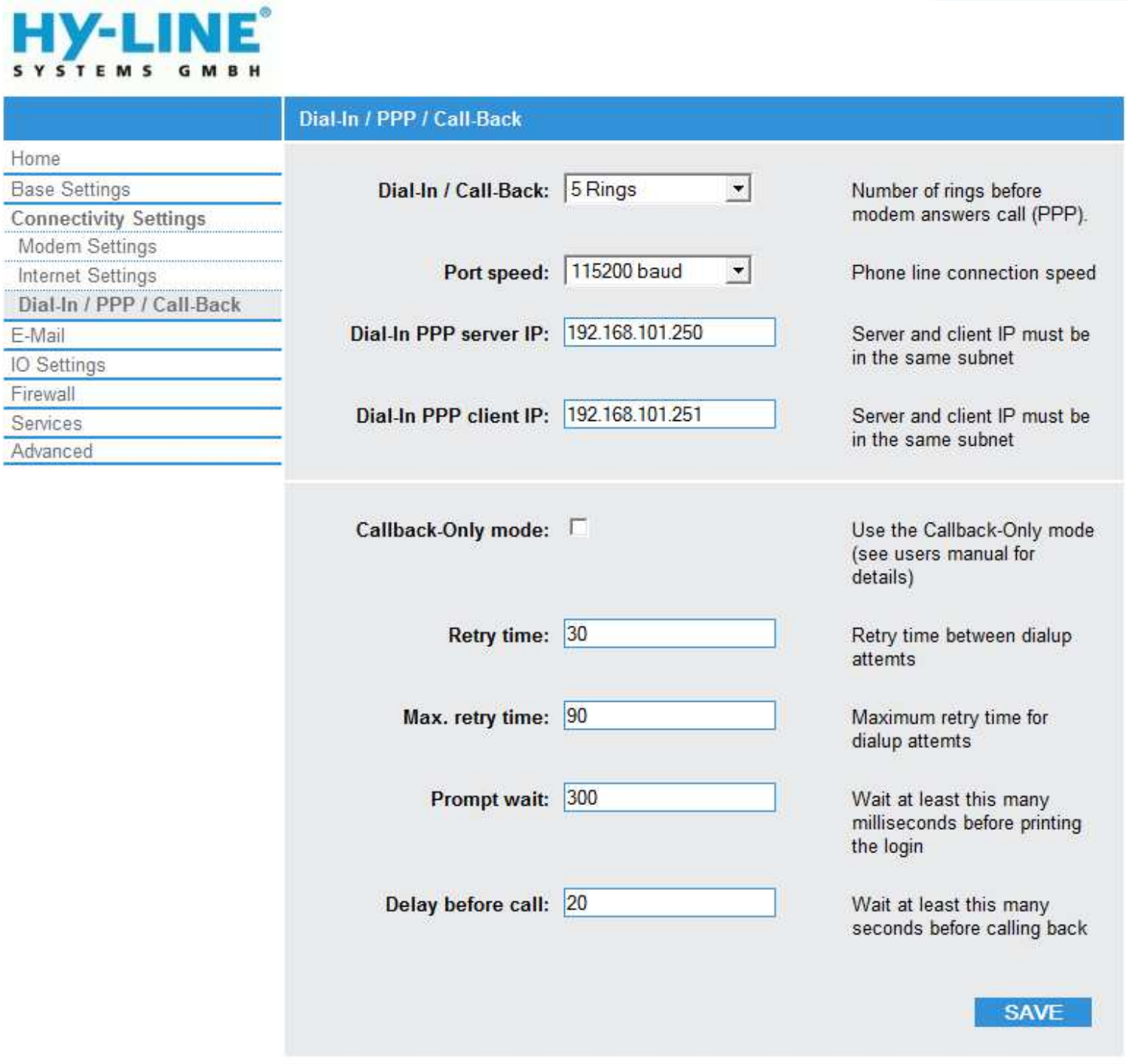
- Rdate (RFC868): die Zeit wird einmal nach dem Online gehen aktualisiert
- NTP (RFC 1305): die Zeit wird fortlaufend synchronisiert (bitte den entstehenden Traffic beachten)



- **Network connection mode:** Internet Einwahl:
  - On-Demand: nach Bedarf, Timeout Funktion aktiv
  - Persistent: permanent (zusätzlich InetWD Service aktivieren)

- **Use peer DNS:** Übernahme der DNS-Adresse vom Provider bei der Internet Einwahl

Connectivity Settings – Dial-In / Call Back:



- **PPP-Einwahl (Dial-In):** Der Router nimmt nach den eingestellten Klingeltönen ab und die PPP-Verbindung wird aufgebaut. Nach Trennen der PPP-Verbindung sollte ca. 30 Sekunden gewartet werden, bis eine erneute PPP-Verbindung zum Router aufgebaut wird.

Connectivity Settings – Dial-In / Call Back:

- **Internet by Call Einwahl / Anklingel-Funktion:** Anklingeln des M2M Routers von Festnetz, Handy oder PC-Modem aus veranlasst den Router sich im Internet einzuwählen (über den voreingestellten Internet-Provider bei Internet Settings).

- **Port Speed:** bei schlechten Analogleitungen (oft im Ausland) kann hier die Geschwindigkeit der Datenkommunikation verringert werden

- **Dial-In Server/Client IP:** IP-Adressen des PPP-Tunnels, sollten im gleichen Subnetz liegen wie das Gateway (M2M Router IP-Adresse). Vorteil: Die Router IP muß nicht als Gateway in den IP-Geräten eingetragen werden.

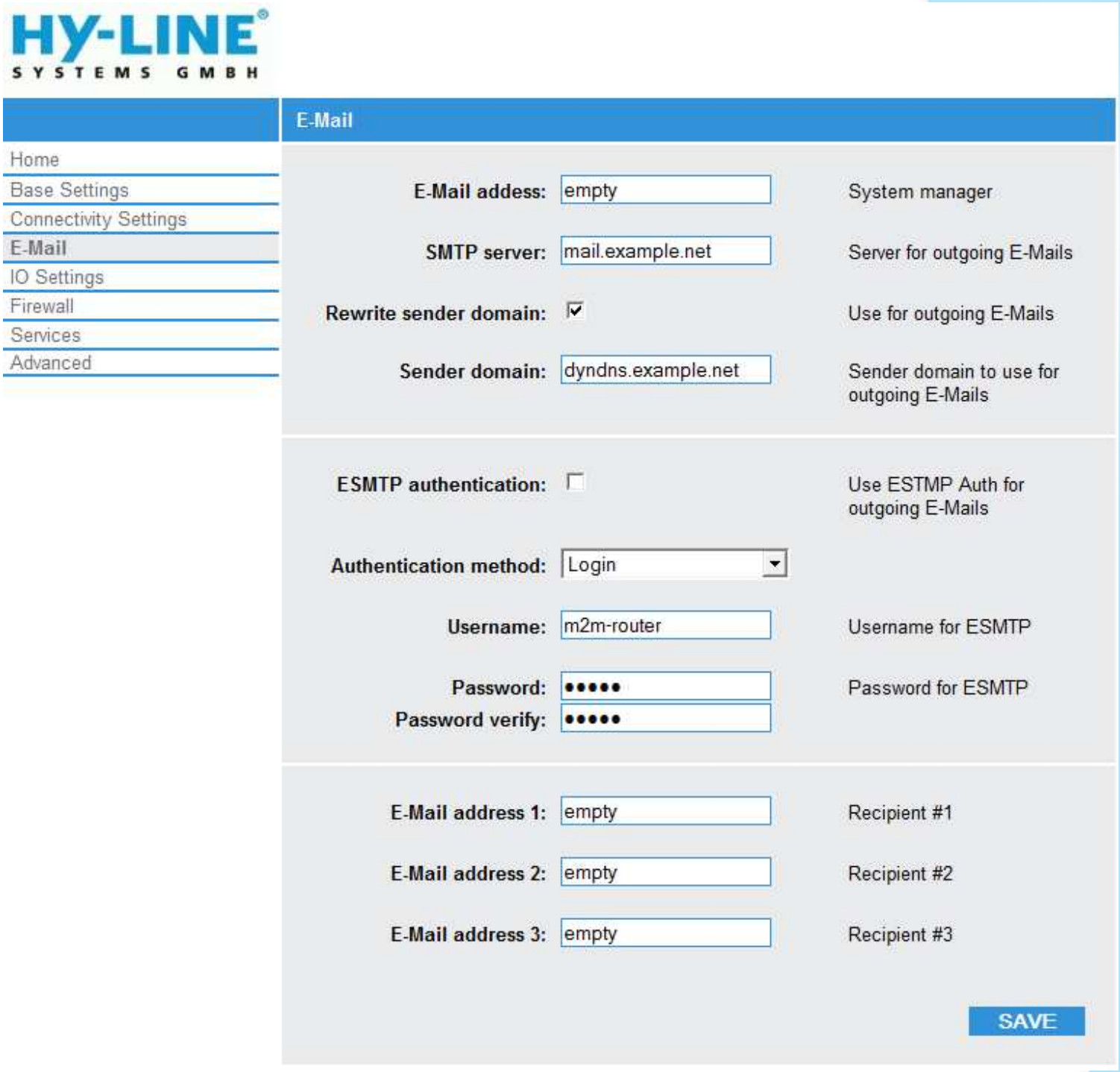
Konfiguration PPP-Direkteinwahl im M2M Router:

Im Auslieferungszustand ist ein PPP-Benutzer (siehe unten) auf dem Router angelegt. Dieser wird im User Management nicht angezeigt. Es können weitere PPP-Benutzer als System User angelegt werden.

PPP-Einwahl:
-Benutzername: pppuser
-Passwort: M2MLogin (Groß-Kleinschreibung beachten)
-DFÜ-Client Einstellung: Windows Standard Einstellungen für DFÜ-Clients übernehmen
Das Passwort kann geändert werden, hier müssen Sie unter der Rubrik System user dem Benutzer pppuser ein anderes Passwort vergeben.

Wichtig: Bitte überprüfen Sie im User-Management, dass hier keine User angelegt sind mit dem Namen: pppuser. Wenn doch, löschen Sie diesen aus allen User-Kategorien.

E-Mail:


HY-LINE SYSTEMS GMBH
Home
Base Settings
Connectivity Settings
E-Mail
IO Settings
Firewall
Services
Advanced
E-Mail
E-Mail addess: empty
System manager
SMTP server: mail.example.net
Server for outgoing E-Mails
Rewrite sender domain:
Use for outgoing E-Mails
Sender domain: dyndns.example.net
Sender domain to use for outgoing E-Mails
ESMTP authentication:
Use ESTMP Auth for outgoing E-Mails
Authentication method: Login
Username: m2m-router
Username for ESMTP
Password: •••••
Password verify: •••••
Password for ESMTP
E-Mail address 1: empty
Recipient #1
E-Mail address 2: empty
Recipient #2
E-Mail address 3: empty
Recipient #3
SAVE

E-Mail:

- **E-Mail address:** E-Mail Adresse des System Managers, kann als Admininstrator eingesetzt werden, der im Bedarfsfall alle E-Mails bekommt (als Kopie)

- **SMTP-Server:** Adresse des SMTP-Server zum Senden von E-Mails (unterstützt Rechner-Namen und IP-Adressen)

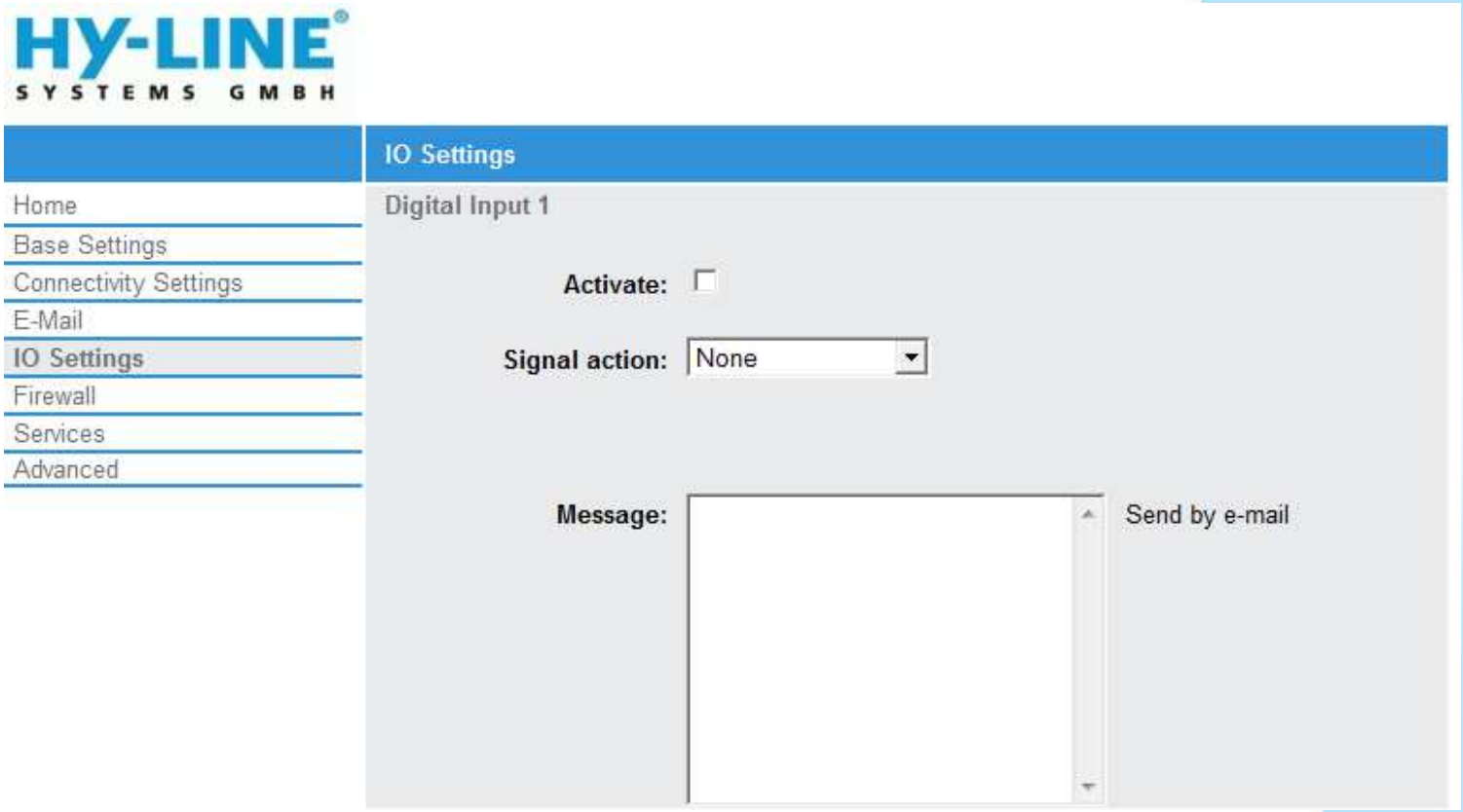
- **Rewrite sender domain:** zum Senden von E-Mails wird die Übermittlung der angegeben Domain verwendet

- **Sender domain:** Absenderdomain der E-Mails (die Absenderdomain muß eine gültige Domain sein)

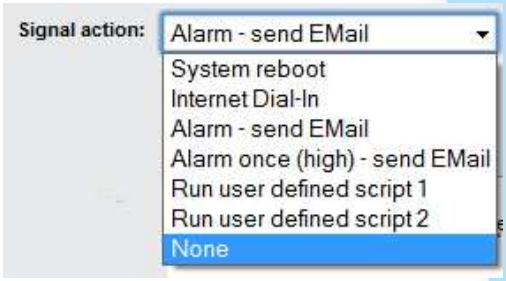
- **ESMTP authentication:** Aktivieren, wenn der SMTP Server zum Senden von E-Mail eine Authentifizierung benötigt

- **E-Mail address 1-3:** E-Mail Empfänger 1-3

I/O-Settings – Digital Input / Output:

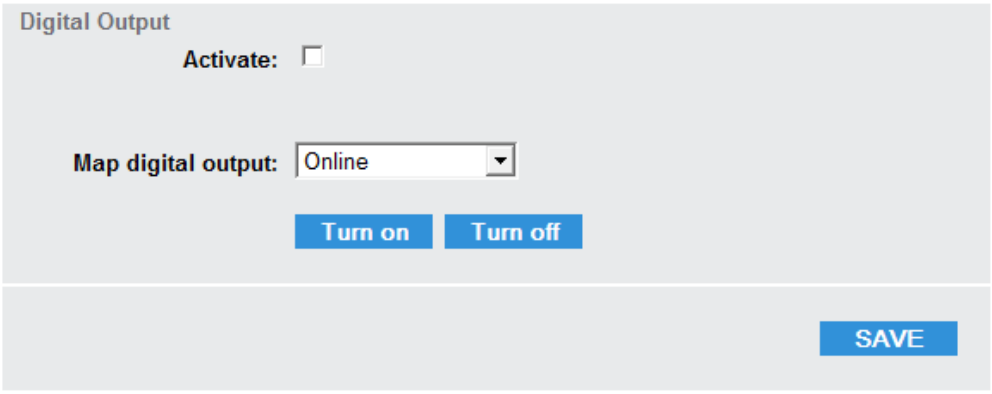


- **Activate:** Aktivierung der Überwachung der digitalen Eingänge 1/2
- **Signal action:**



- *System reboot*: Neustart des Routers (Softreset)
- *Internet dial-in:* Einwahl des Routers ins Internet
- *Alarm send E-Mail*: Versenden einer E-Mail an Empfänger 1-3 mit Benachrichtigungstext (Message)
- *Alarm once (high) send Email*: Versenden einer E-Mail an Empfänger 1-3 und System Manager mit Benachrichtigungstext (Message) nach Neustart des Routers bei gleichzeitig anliegendem High-Signal an DigEin (muß während des Boot Vorgangs anliegen) Die Mail wird einmal gesendet, im laufenden Betrieb ist dann kein Senden über den DigEin1 triggerbar
- *Run user defined script 1/2:* Ausführen von selbst erstellten Linux Scripten. Die (leeren) Scripte sind vorhanden und liegen unter ../usr/sbin und heißen "user1.sh" und "user2.sh". Wenn man die Dateien editiert, müssen ‚execute' Rechte/Attribute nach dem Editieren für die Dateien neu gesetzt werden.

I/O-Settings – Digital Input / Output:



- **Activate:** Aktivierung der Funktion des digitalen Ausganges
- **Map digital output:** Der aktuelle DigEin1, DigEin2 oder Online Status wird auf den Ausgang abgebildet
- **Turn On / Turn off:** manuelles Ein- und Ausschalten des Digitalausgangs

Technische Daten zu den Digital I/Os:

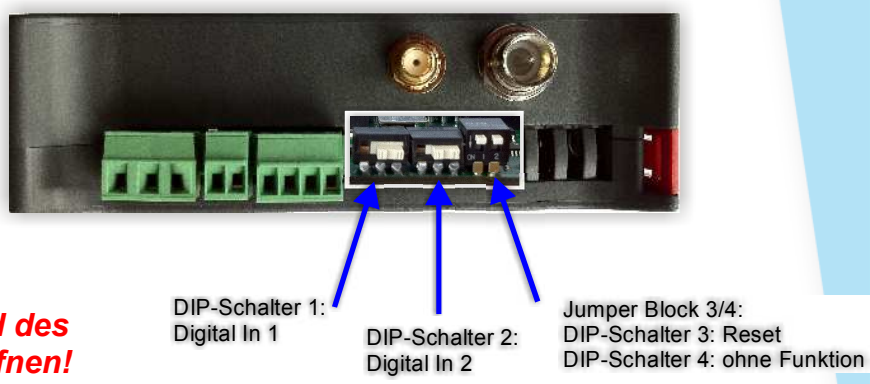
- Aus **EMV** Konformitätsgründen müssen Digitalleitungen, die länger als 3m sind, mit einem Ferrit Kern versehen werden (nur notwendig bei UMTS Routern). Folgende Ferritkern eignet sich hierfür: *Würth 74270090 mit zwei Windungen*

- **Digital Eingang 1 / 2: Standardkonfiguration / Auslieferungszustand: Potentialfreie Eingänge:** triggern auf Flankenänderung High-Low Pegeländerung, mittels DIP-Schalter (Position siehe Bild: Router Gehäuse Seite, hinter Lüftungsgitter auf Seite der Spannungsversorgung) lassen sich die Eingänge als potentialfreie Eingänge konfigurieren. Hierfür DIP-Schalter 1, für DigEin1 und Dip-Schalter 2, für DigEin2, in folgende Position bringen: weg von den grünen Buchsen hin gestellt, siehe Bild (Auslieferungszustand).

- **Digital Eingang 1 / 2: Impulseingang**: triggern auf Flankenänderung High-Low Pegeländerung, Überwachung von Aktiv-High Signalen, Schalteingangsspannung max. 24VDC/ min. 5mA. Hierfür DIP-Schalter 1, für DigEin1 und Dip-Schalter 2, für DigEin2, in folgende Position bringen: zu den grünen Buchsen hin gestellt, Lage siehe Bild.

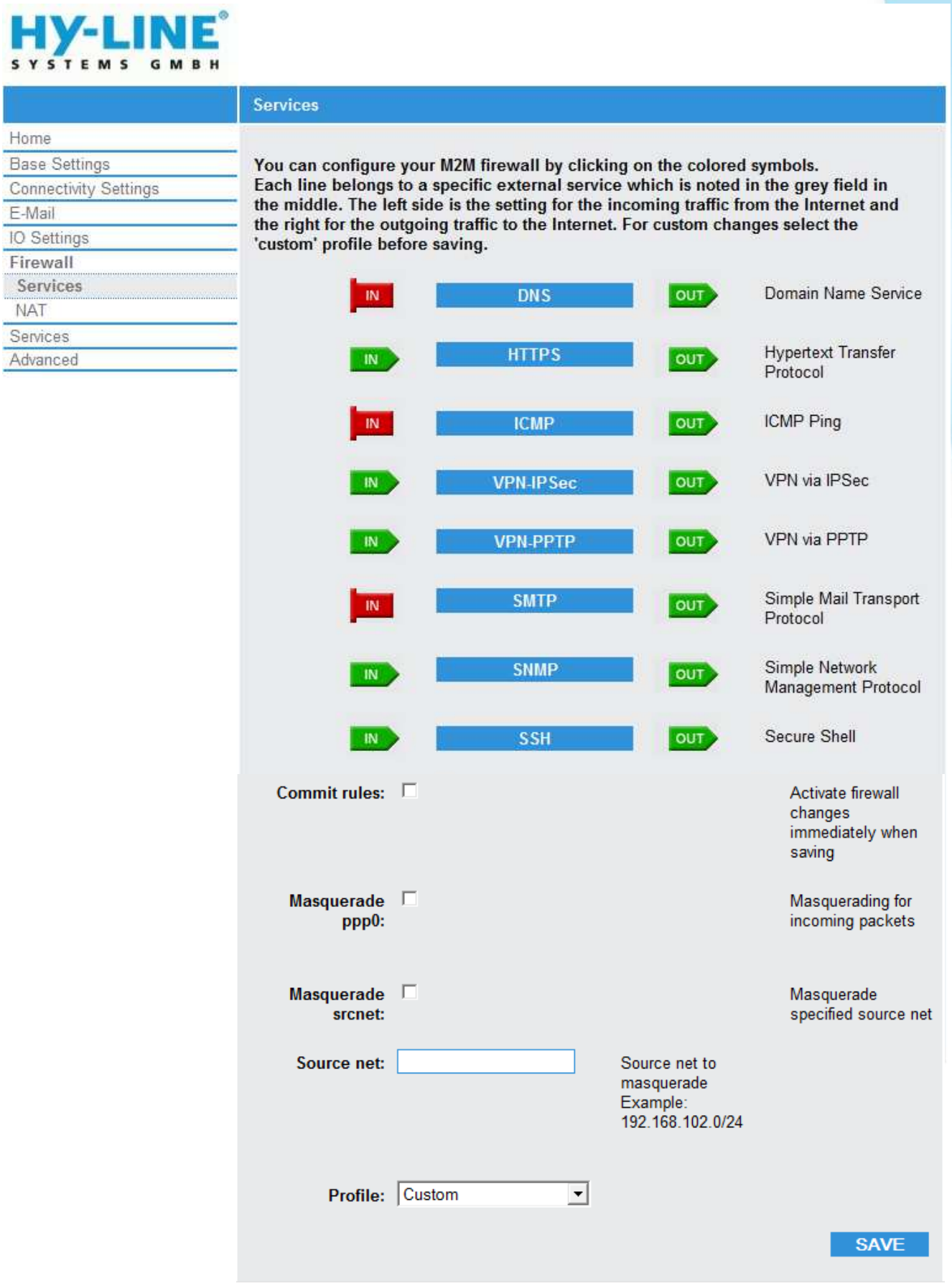
- **Digital Ausgang:** Open Collector: Ausgangsspannung 12-30VDC (aktiv) / max. 100mA. Die Ausgangsspannung entspricht der am Router angelegten Versorgungsspannung.

Die Position der Jumper (hinter den Lüftungsschlitzen) im Bild zeigt die Konfiguration (Auslieferungszustand) von DigEin1 und DigEin2 als potentialfreie Eingänge.



Bei Konfiguration potentialfreie Eingänge darf nicht mit einer Spannung geschaltet werden!
Die Jumper nur im ausgeschalteten Zustand des Routers setzen. Das Gehäuse dafür nicht öffnen!

Firewall:


HY-LINE SYSTEMS GMBH
Home
Base Settings
Connectivity Settings
E-Mail
IO Settings
Firewall
Services
NAT
Services
Advanced
Services
You can configure your M2M firewall by clicking on the colored symbols. Each line belongs to a specific external service which is noted in the grey field in the middle. The left side is the setting for the incoming traffic from the Internet and the right for the outgoing traffic to the Internet. For custom changes select the 'custom' profile before saving.
IN DNS OUT Domain Name Service
IN HTTPS OUT Hypertext Transfer Protocol
IN ICMP OUT ICMP Ping
IN VPN-IPSec OUT VPN via IPSec
IN VPN-PPTP OUT VPN via PPTP
IN SMTP OUT Simple Mail Transport Protocol
IN SNMP OUT Simple Network Management Protocol
IN SSH OUT Secure Shell
Commit rules:
Activate firewall changes immediately when saving
Masquerade ppp0:
Masquerading for incoming packets
Masquerade srcnet:
Masquerade specified source net
Source net:
Source net to masquerade Example: 192.168.102.0/24
Profile:
Custom
SAVE

Fortsetz.: Firewall:

Die **Firewall Konfiguration** erlaubt die Freigabe/Sperre verschiedener Dienste vom Internet zum Router (Pfeile links) und vom Router zum Internet (Pfeile rechts)

Drei verschiedene Standard Profile stehen zur Verfügung:

- *Default* – Standard, für die meisten Anwendungen empfehlenswert
- *Custom* – Benutzer angepasstes Profil, dieses muß gewählt werden, falls Änderungen vom Benutzer gemacht wurden
- *Minimum* – hohe Sicherheitseinstellungen

- **Commit rules:** Änderungen an den Firewall Einstellungen werden bei Aktivierung der Funktion direkt nach SAVE übernommen, ansonsten erst bei Neustart des Routers.

- **Masquerading:** Eingehende Pakete in den Router werden mit der Router-LAN IP-Adresse maskiert (als Absenderadresse). Man spricht auch von SNAT. Der Router schreibt von ppp0 einkommende Pakete so um, dass er sich selbst als Absender einträgt. Am Zielgerät kommt ein Paket vom Router an, die ursprüngliche Absenderaddresse ist nicht mehr sichtbar.

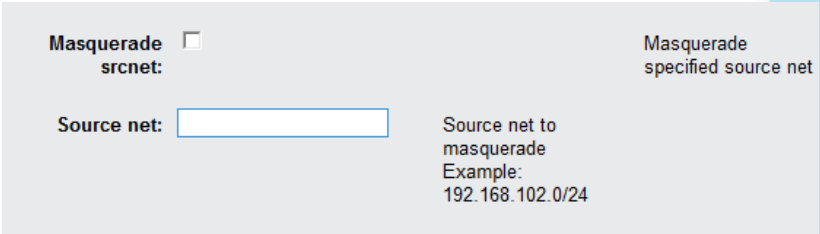
Kommt daraufhin eine Antwort, erkennt der Router, dass das eine Antwort auf ein SNAT Paket ist und ersetzt in der Zieladdresse seine eigene durch die ursprüngliche und schickt das Paket weiter nach außen.

Praktisch gesehen, kommen bei dem Gerät hinter dem HY-LINE Router alle ge-NATeten Pakete mit einer Sourceadresse vom Router an. Damit muß man u.a. auf diesem Gerät keine Defaultroute setzen, da die Antworten schon "automatisch" an den Router gehen.

Ausgehende Verbindungen (HY-LINE Router LAN -> externe Gateway) :

- **Masquerade srcnet:** Aktivieren: erlaubt ausgehende TCP-Pakete über ein Standard Gateway (keine Modemgateway)

- **Source net:** Netzmaske/IP-Bereich des zu ausgehenden Traffic Format: 192.168.102.0/24 (Beispiel) Siehe Seite 17.



Proxy-ARP:

Der Proxy-ARP ist im Standard aktiviert. Deaktiviert wird dieser über einen Eintrag in der Datei: ../etc/amsel/system.conf Diese Änderung kann nicht über das Webinterface erfolgen, einzig über die Linux Shell Ebene.

ProxyArp aktiviert:
"echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy_arp";

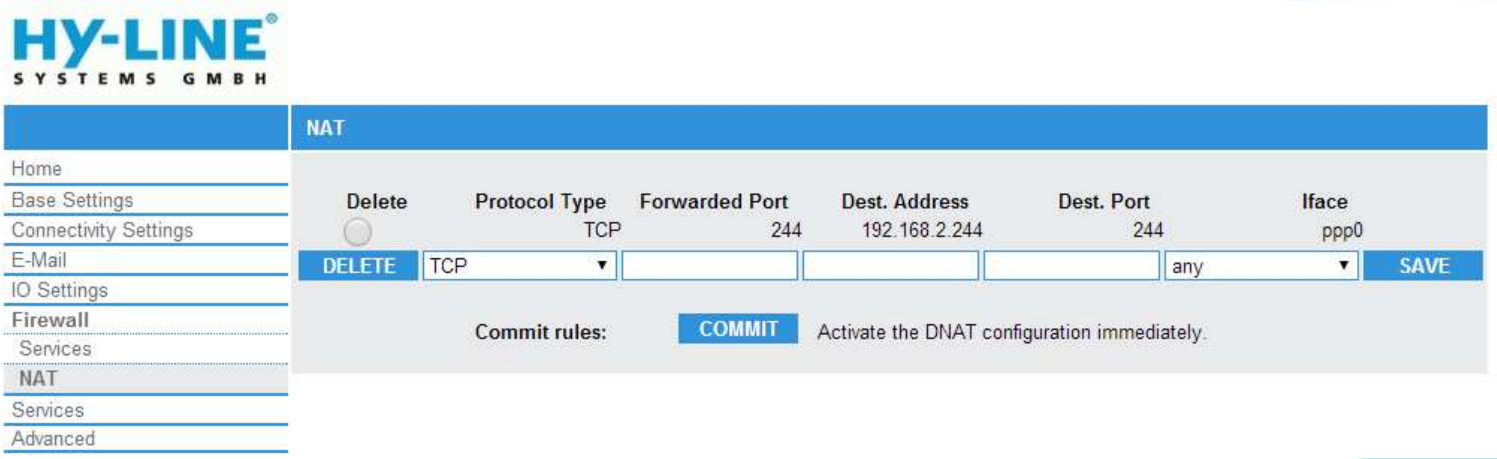
ProxyArp de-aktiviert:
"echo 0 > /proc/sys/net/ipv4/conf/eth0/proxy_arp";

NAT (Network Address Translation)

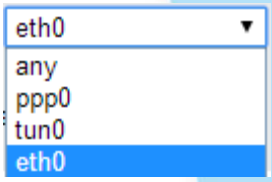
Der HY-LINE Router unterstützt Portweiterleitung, auch **Destination NAT (D-NAT)** genannt. Über das Webinterface können max. 150 NAT-Regeln angelegt werden.

Eine **Portweiterleitung** (engl. *port forwarding*) beschreibt die Möglichkeit, eine über Netzwerk eingehende Verbindung auf einen bestimmten Port zu einem anderen Computer innerhalb eines Netzes weiterzuleiten.
Die eingehenden Datenpakete werden hierbei per *Destination NAT* und die ausgehenden Pakete per *Source NAT* maskiert.

Konfiguration über Webseite:



- **Protocol Type:** Auswahl des Protokolls TCP oder UDP
- **Forwarded Port:** Weiterzuleitender Port
- **Dest. Address:** IP-Zieladdresse des Geräts im Router Netz, auf den die Daten geschickt werden
- **Dest. Port:** Zielport des Geräts im Router-Netz, auf den die Daten geschickt werden



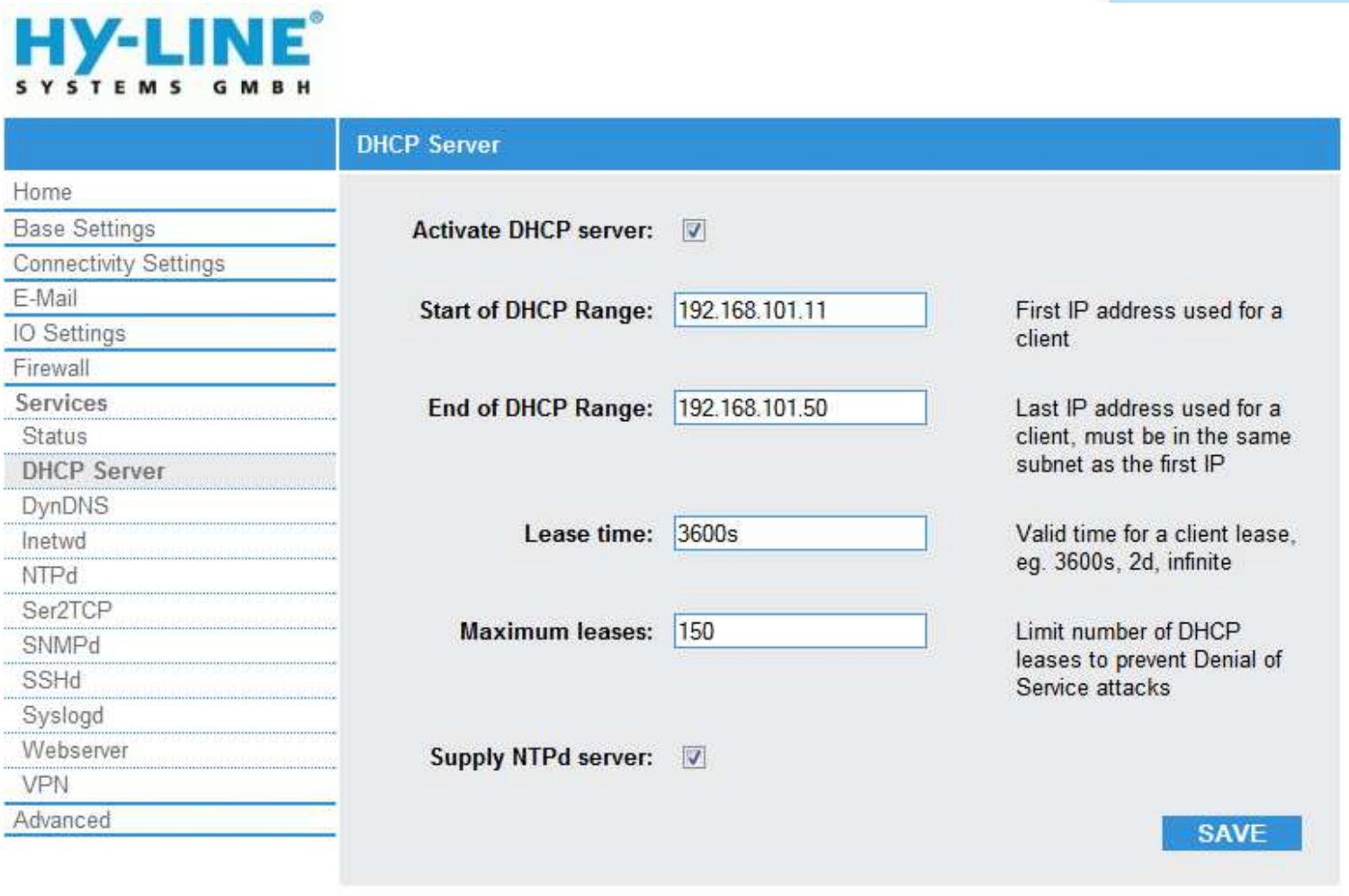
- **Iface:** Interface, auf welche die NAT Regel aktiv ist: any=alle; eth0=lan0/1/2; ppp0=WAN/Internet; tun0=VPN-Tunnel – NAT Regelen werden logisch UND verknüpft.
- **Commit rules:** Sofortiges Übernehmen und Aktivieren der NAT-Regeln beim Speichern. Ansonsten ist ein Neustart erforderlich.

Dienst/Anwendung	Protokoll	Port
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP) HTTPS	TCP TCP	80 443
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631

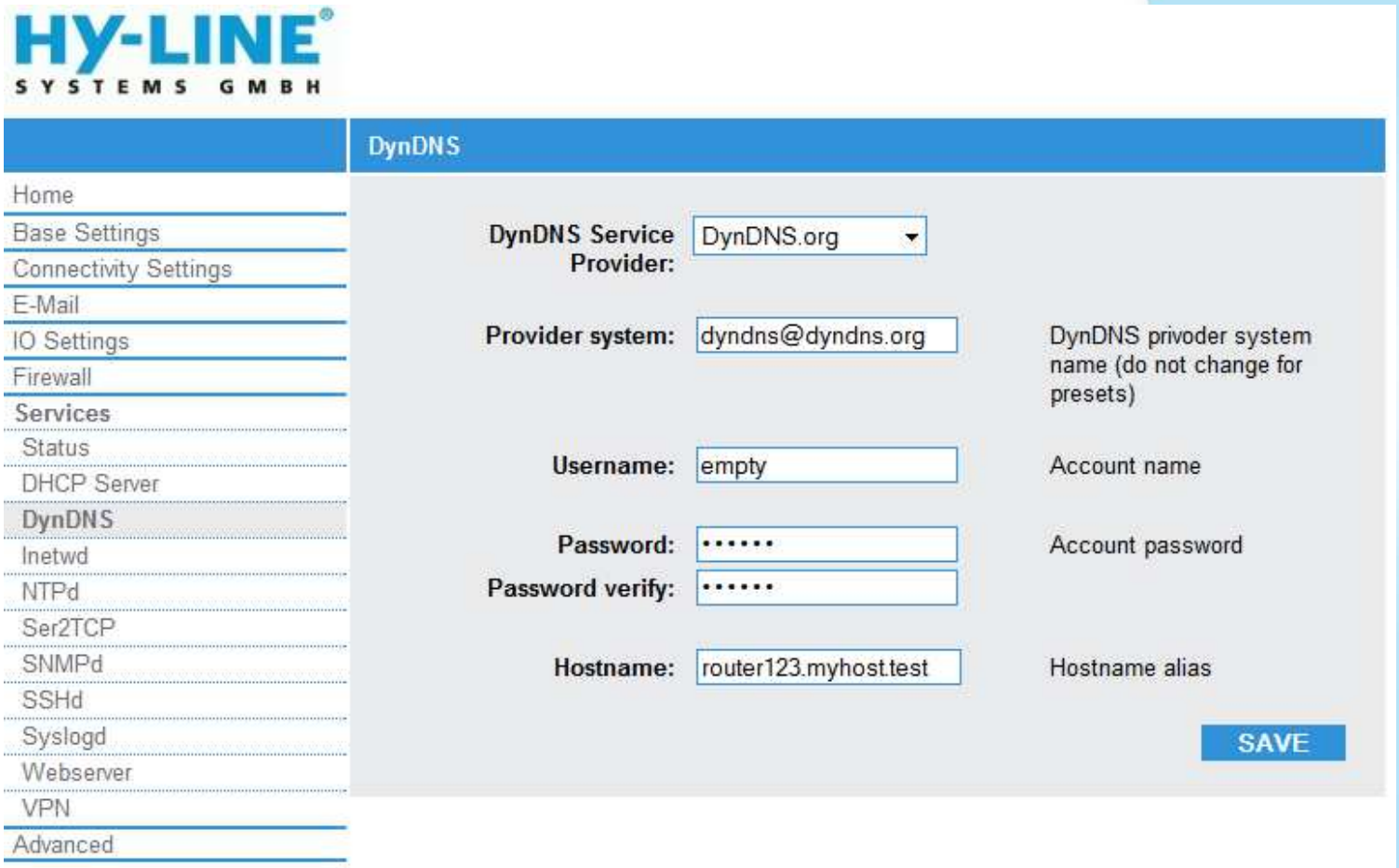
Services - Status:

Über das Service Menü lassen sich Dienste wie z.B. DHCP, abschalten, stoppen und starten.

Services - DHCP/DNS Server:



Services - DynDNS:

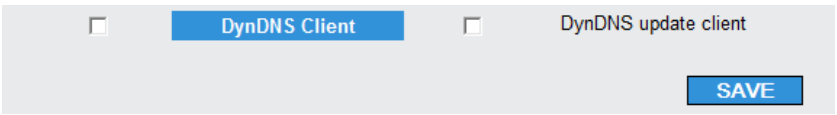


- **DynDNS Service Provider:** Auswahl des Providers zur Nutzung des DynDNS Servers. Hier stehen mehrere Provider zur Verfügung
- **Username:** Benutzername für DynDNS Server Zugang
- **Passwort:** Passwort für DynDNS Server Zugang
- **Passwort verify:** Passwort Bestätigung für DynDNS Server Zugang
- **Host alias:** DynDNS Hostname

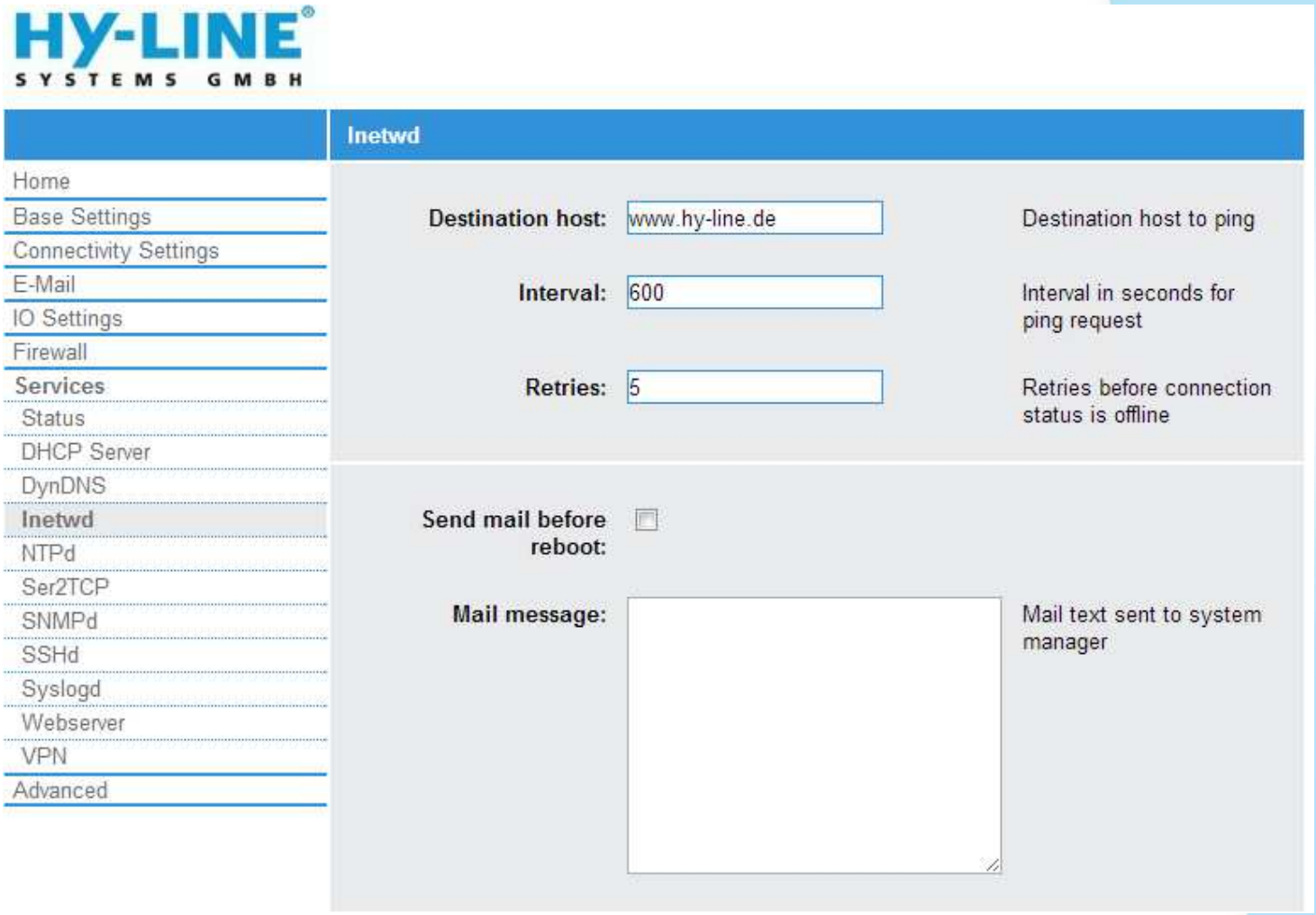
Einschalten des DynDNS Services

Modem-Betrieb:
Der DynDNS Dienst muß im Menü ../Connectivity Settings/Internet Settings/ unter IP-Reporting mode aktiviert werden!

Gateway Betrieb:
Aktivieren des DynDNS Dienst im Service Menü:



Services - Inetwd + Redundancy:



Funktionsweise Internet Watchdog (Inetwd):

Der **Internet Watchdog Service** überprüft mittels PING (icmp-Protokoll) in zyklischen Abständen, ob eine IP-Adresse oder Hostname im Internet erreichbar ist. Ist die IP-Adresse oder Hostname nicht erreichbar, wird versucht eine neue Interneteinwahl herzustellen. Diese Funktion ist wichtig bei Routern die permanent (Always Online) mit dem Internet verbunden sein sollen.

Zu beachten: aktiviert erzeugt diese Funktion Datenvolumen durch den ping, ca. 32Byte pro Ping, Menge je nach Einstellung: default, alle 600 Sekunden.

- **Destination host:** IP-Adresse oder Hostname im Format: www.name.endung
- **Interval:** Wartezeit in Sekunden zwischen den ping Versuchen
- **Retries:** Anzahl der Versuche den Host zu erreichen.

Send mail before reboot: vor Neustart des Routers (getriggert durch den Internet Watchdog) wird ein Mail an den System manager verschickt

Funktionsweise Redundancy: redundanter Kommunikationsweg

a) LAN-Gateway (DHCP) → UMTS / PPPoE (intern DSL oder externes Modem)

Der Router ist nur über die aktuell aktive Verbindung online. Der primäre, aktive Kommunikationsweg (nach Router Reboot) ist immer LAN-Gateway (DHCP).

Sobald der primäre, aktive Kommunikationsweg ausgefallen ist, wird die Kommunikation automatisch auf den redundanten Kommunikationsweg (UMTS/PPPoE) aktiviert. Diese Funktion wird durch den Dienst InetWD aktiviert. Anschließend wird der DHCP Dienst (falls aktiviert) beendet und der Router neu gestartet. Nach dem Neustart ist der aktive Kommunikationsweg UMTS/PPPoE. Es wird eine E-Mail abgesetzt, die eine (definierbare) Information enthält.

Umschalten auf den primären Kommunikationsweg erfolgt manuell über die Router Weboberfläche, einfach durch einen Reboot/ Neustart des Routers (übers Internet oder Intranet).

b) LAN-Gateway (kein DHCP) → LAN-Gateway (kein DHCP)

Funktionsweise redundanter Kommunikationsweg, wie unter a).

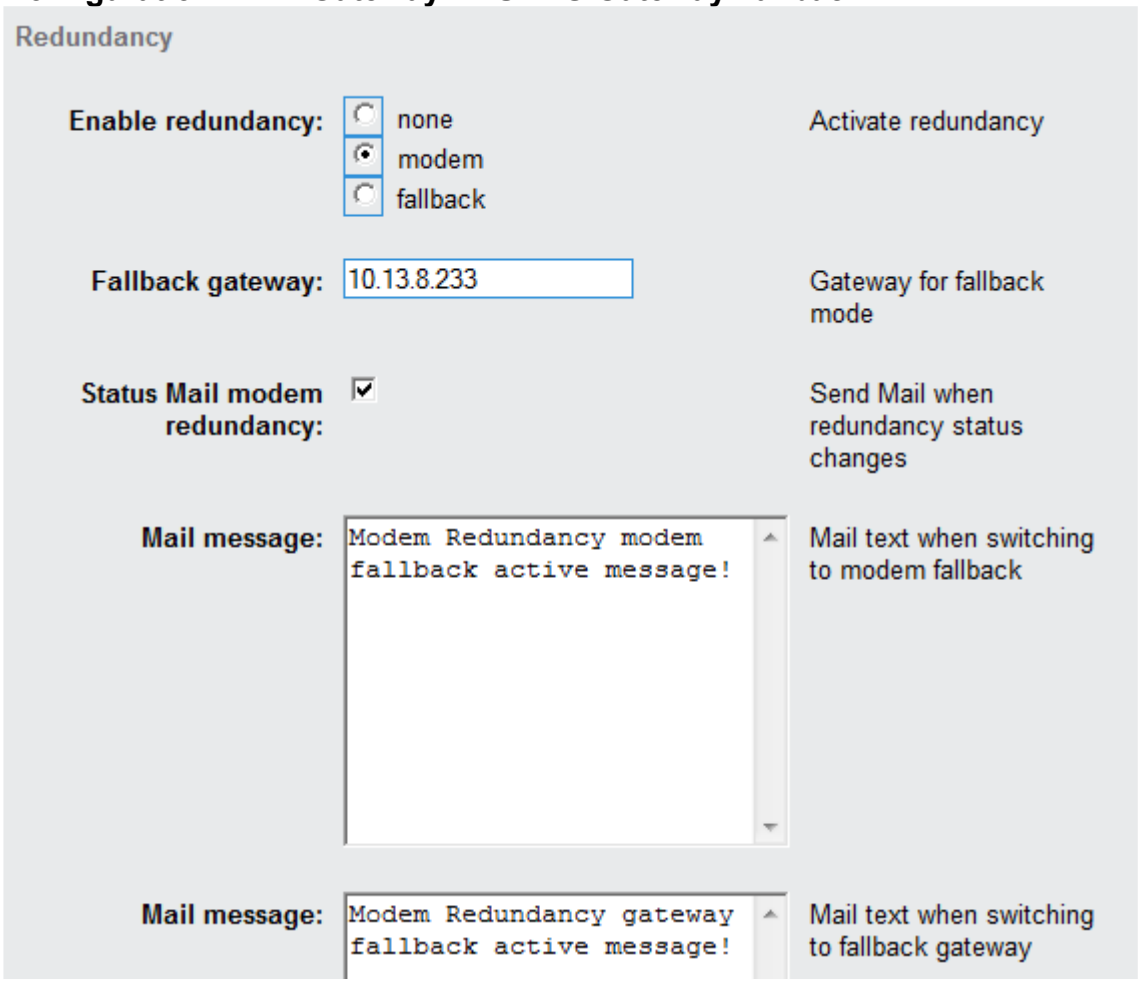
Voraussetzung: es darf kein DHCP Client bei den LAN Einstellungen im Router aktiviert sein, alle LAN-Parameter müssen manuell eingegeben werden.

Das Umschalten auf den primären Kommunikationsweg/ Gateway erfolgt manuell über die Router Weboberfläche durch einen Reboot/ Neustart des Routers (übers Internet oder Intranet).

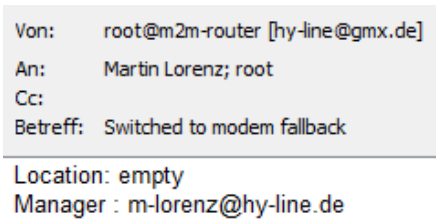
Das Umschalten des aktiven Gateways nach erfolglosem Ping des InetWD automatisch auf das redundanten Gateway.

Fortsetz.: Services - Redundancy

Konfiguration: LAN-Gateway –> UMTS/Gateway Fallback



- **Enable redundancy:** Redundanz aktivieren, Optionen: Redundanzweg modem oder Gateway
- **Fallback gateway:** Hier das Gateway im Redundanzfall angeben, das zum Default Gateway wird
- **Status Mail modem r.:** Aktiviert Mail Benachrichtigung im Falle eines umschalten auf den Redundanzweg. Die Mail wird an den system manager verschickt.
- **Mail Message:** Inhalt der Benachrichtigungsmail



Beispiel Redundanz konfigurieren:

- Redundancy aktivieren (modem oder fallback), Mail Benachrichtigung aktivieren und Mail Text angeben

- Service Menü:
- Internet Einwahl auf: Always online
- Internet-Dial-Up Service deaktivieren
- Internet Watchdog Service aktivieren (InetWD)

Fortsetz.: Beispiel Redundanz konfigurieren:

- Konfiguration LAN-Gateway: wie im Kapitel Base Settings / LAN beschrieben vornehmen

DHCP-Server inaktiv im ext. Gateway Subnetz:

LAN 0: Netzwerk/Subnetz auf der der Gateway Seite
LAN 2: Netzwerk/Subnetz des HY-LINE Routers
Gateway (systemwide): Netzwerk/Subnetz auf der der Gateway Seite

DHCP-Server aktiv im ext. Gateway Subnetz:

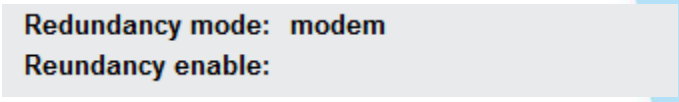
LAN 0: Netzwerk/Subnetz des HY-LINE Routers
LAN 2: Netzwerk/Subnetz auf der der Gateway Seite (DHCP aktivieren)
Gateway (systemwide): Netzwerk/Subnetz auf der der Gateway Seite (wird autom. vergeben)

Konfiguration Firewall:: wie im Kapitel Firewall beschrieben, Masquerading srcnet aktivieren und konfigurieren

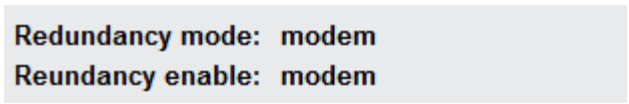
Router Neustart!

- **AKTIVE Redundanz: LAN-Gateway –> UMTS Fallback**

Nach dem Neustart erweitert sich die Anzeige auf der Home Startseite des Routers: es wird eine eingeschaltete Redundanz Funktion angezeigt:



Wir die Redundanz aktiv, d.h. der 2. Kommunikationsweg wird aktiviert, ändert sich die Statusanzeige wie folgt:

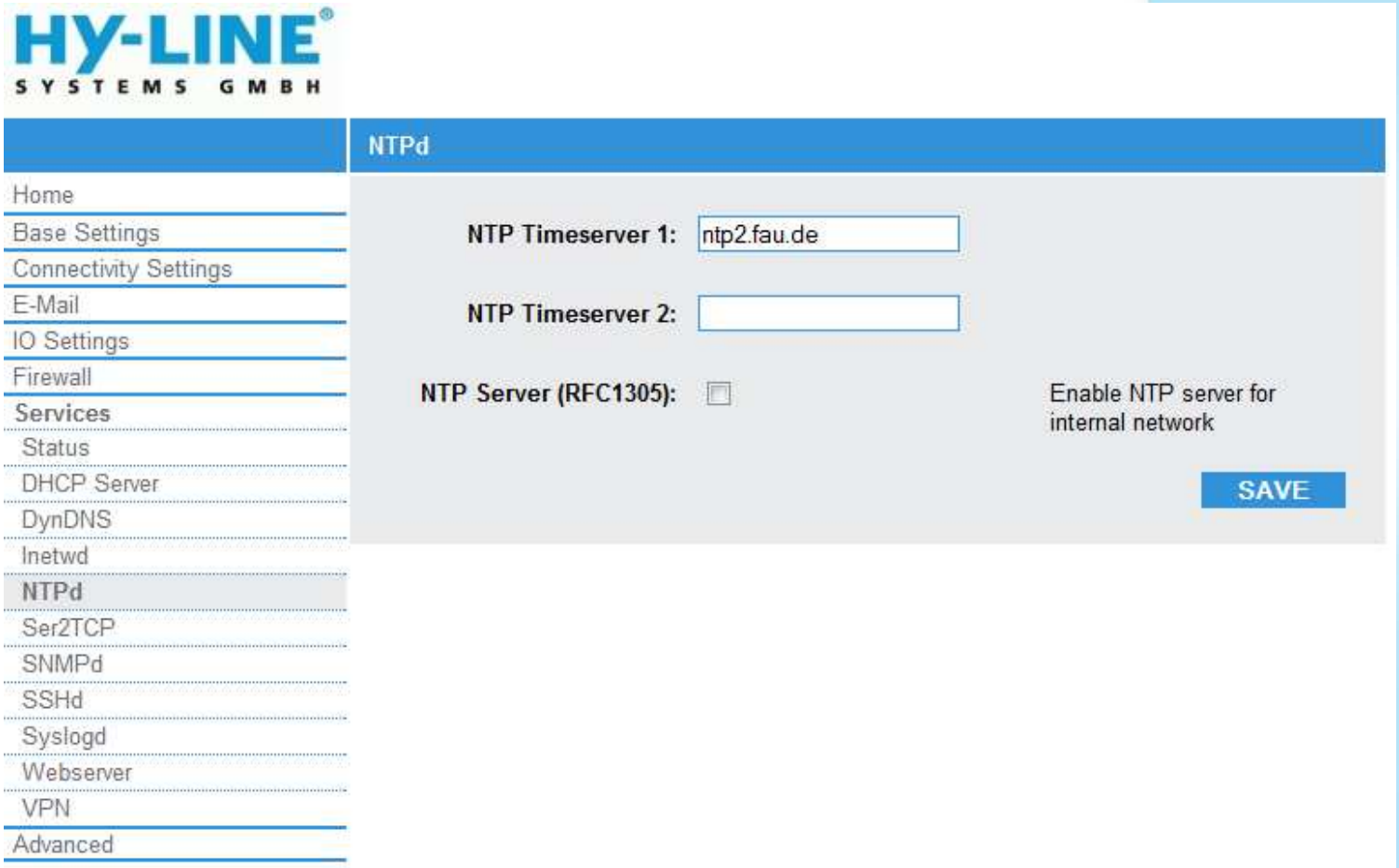


Die erste Zeile zeigt den gewählten Redundanzmodus an, die zweite Zeile zeigt dann denselben Wert an, wenn der inetwd in den Fallback gewechselt hat.

Der inetwd Service läuft nun regulär weiter und versucht (jetzt über den Fallback-Weg) seinen Ping ins Internet abzusetzen. Gelingt das weiterhin nicht, hakt wieder der Reboot ein und das System startet neu (und schaltet damit auf die primäre Funktion zurück).

Nach einem manuellen Reboot des Router über die Webberfläche ist der 1. Kommunikationsweg aktiv.

Services – NTPd Zeitserver:

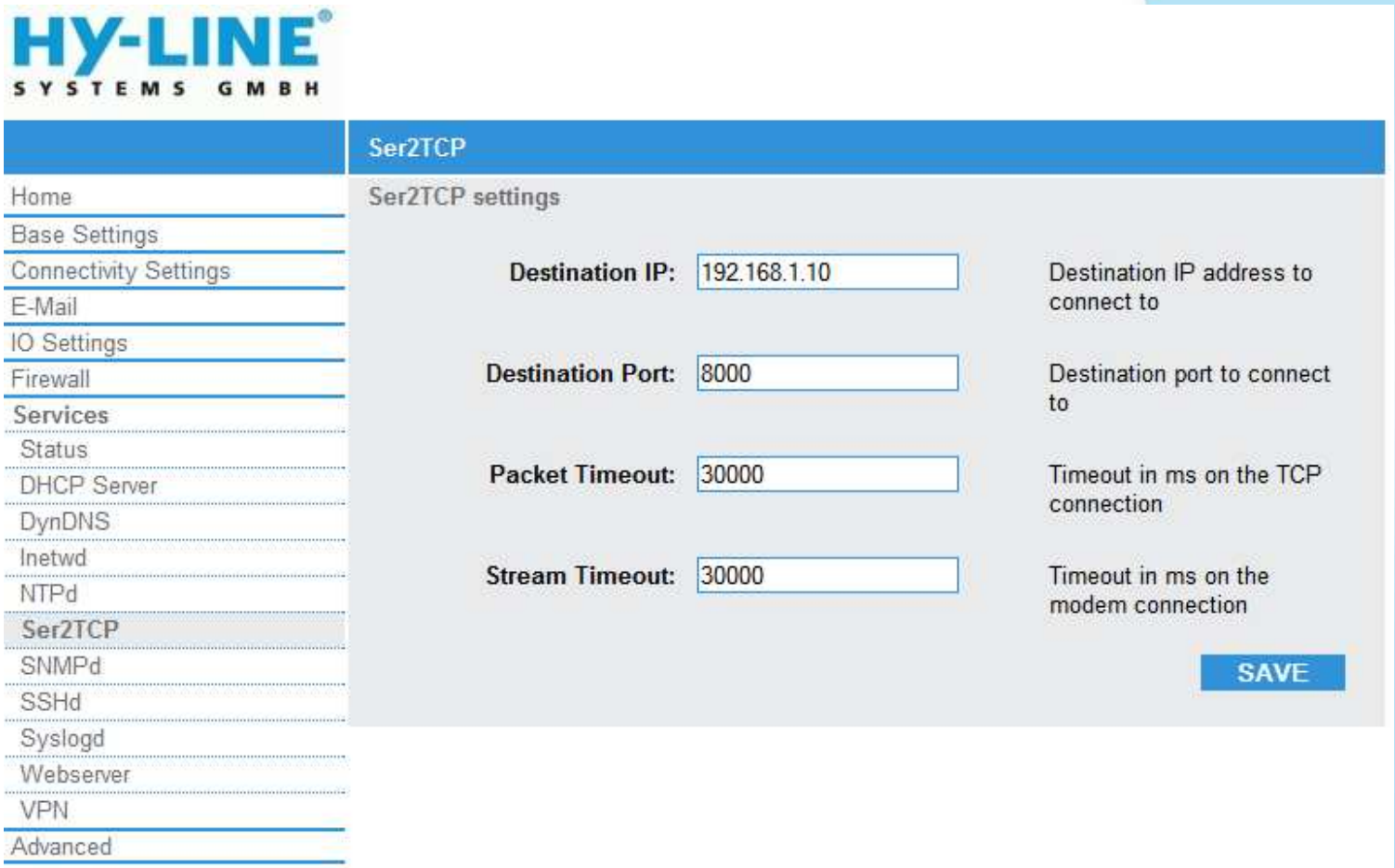


Das Protokoll des Zeitservers ist NTP RFC1305.

- **NTP Timeserver 1/2:** IP Adresse oder Hostname des Zeitservers eintragen. Kann zu Timeserver 1 keine Verbindung aufgebaut werden, wird versucht der Timeserver 2 zu erreichen.

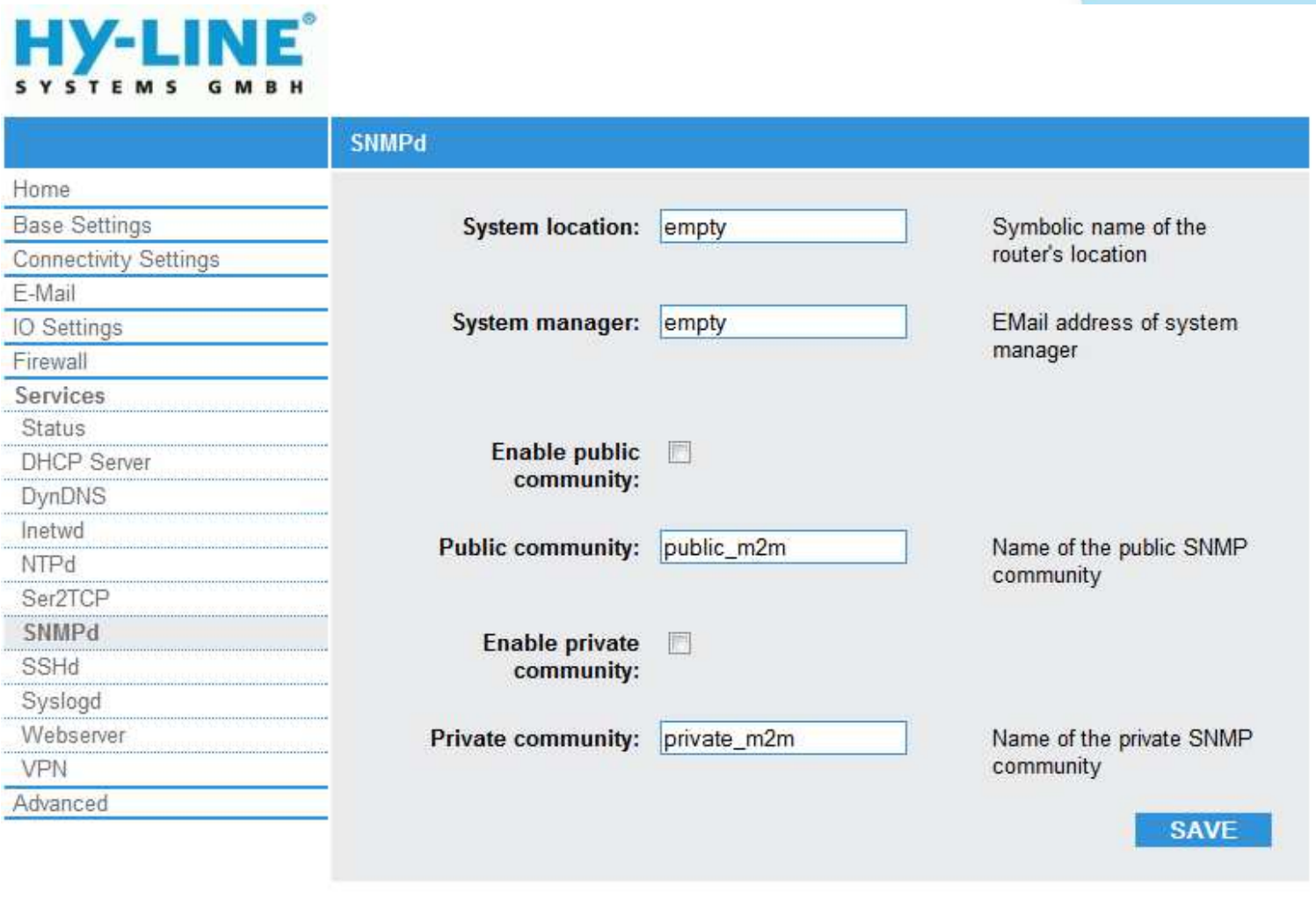
- **NTP Server (RFC 1305):** Aktiviert den NTP Server Modus für das lokale Router Netz. Andere Teilnehmer im lokalen Netzwerk können per NTP Ihre Zeit abgleichen.

Services - Ser2TCP:



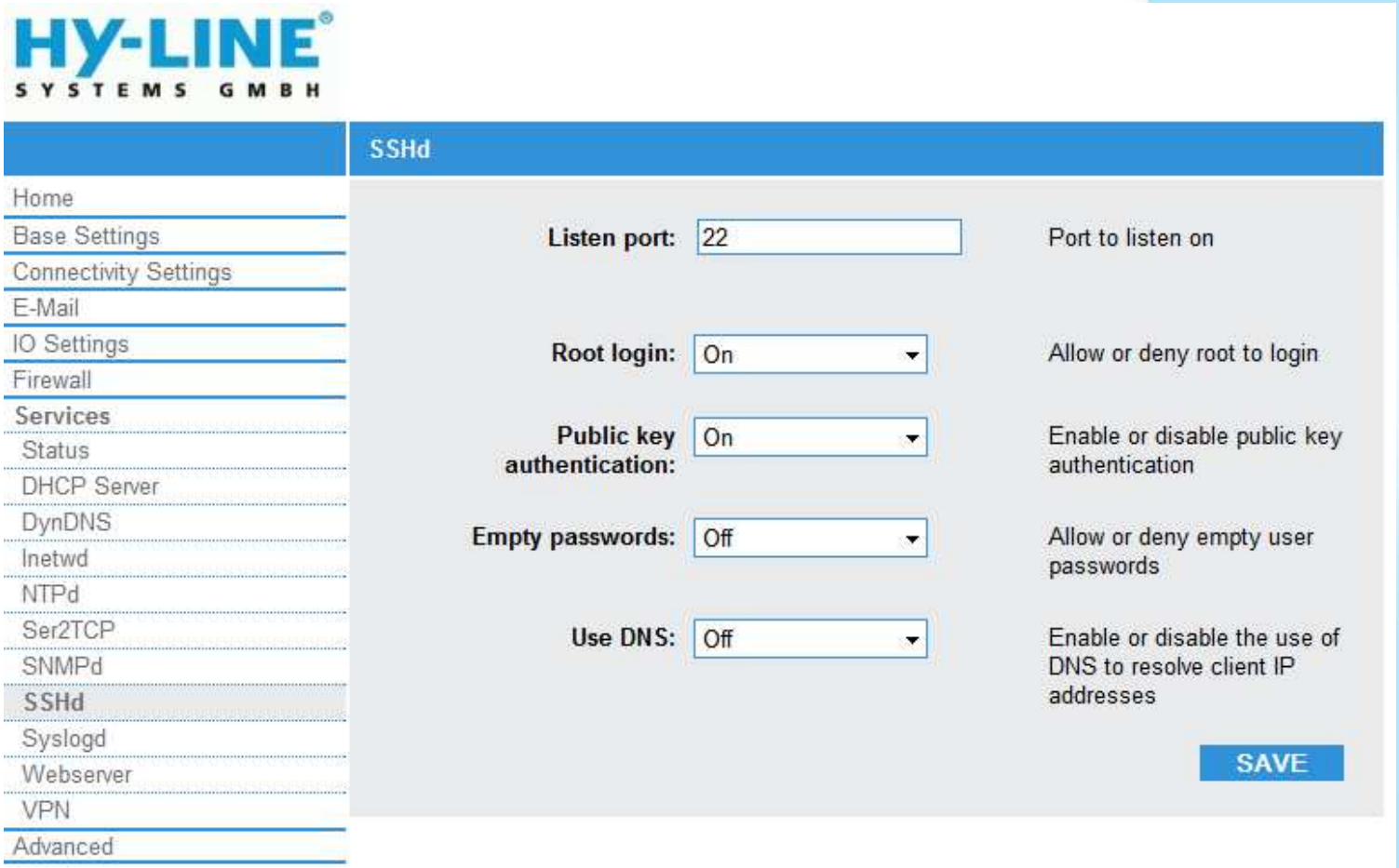
- Der Ser2TCP Dienst erlaubt das Streamen von Daten der seriellen RS232 Router Schnittstelle auf ein Ethernet Gerät im lokalen Router Netzwerk. Es sind erweiterte Einstellungen im Linux OS auf dem Router notwendig. Bei Bedarf wenden Sie sich bitte direkt an den technischen Support von HY-LINE.

Services - SNMP:



- Die MIB Datei (Management Information Base) können Sie beim technischen Support von HY-LINE anfordern!

Services - SSHd:



Menü zum Einstellen des Zugriffes auf den Router per SSH (Secure Shell TCP/IP)

- **Secure Shell -Gesicherte Kommunikation über unsichere Netze**

Secure Shell (ssh) ist ein Programm um über unsichere Netze auf anderen Rechnern zu arbeiten. Es schließt einige Sicherheitslücken, dadurch dass es allen Netzverkehr verschlüsselt.

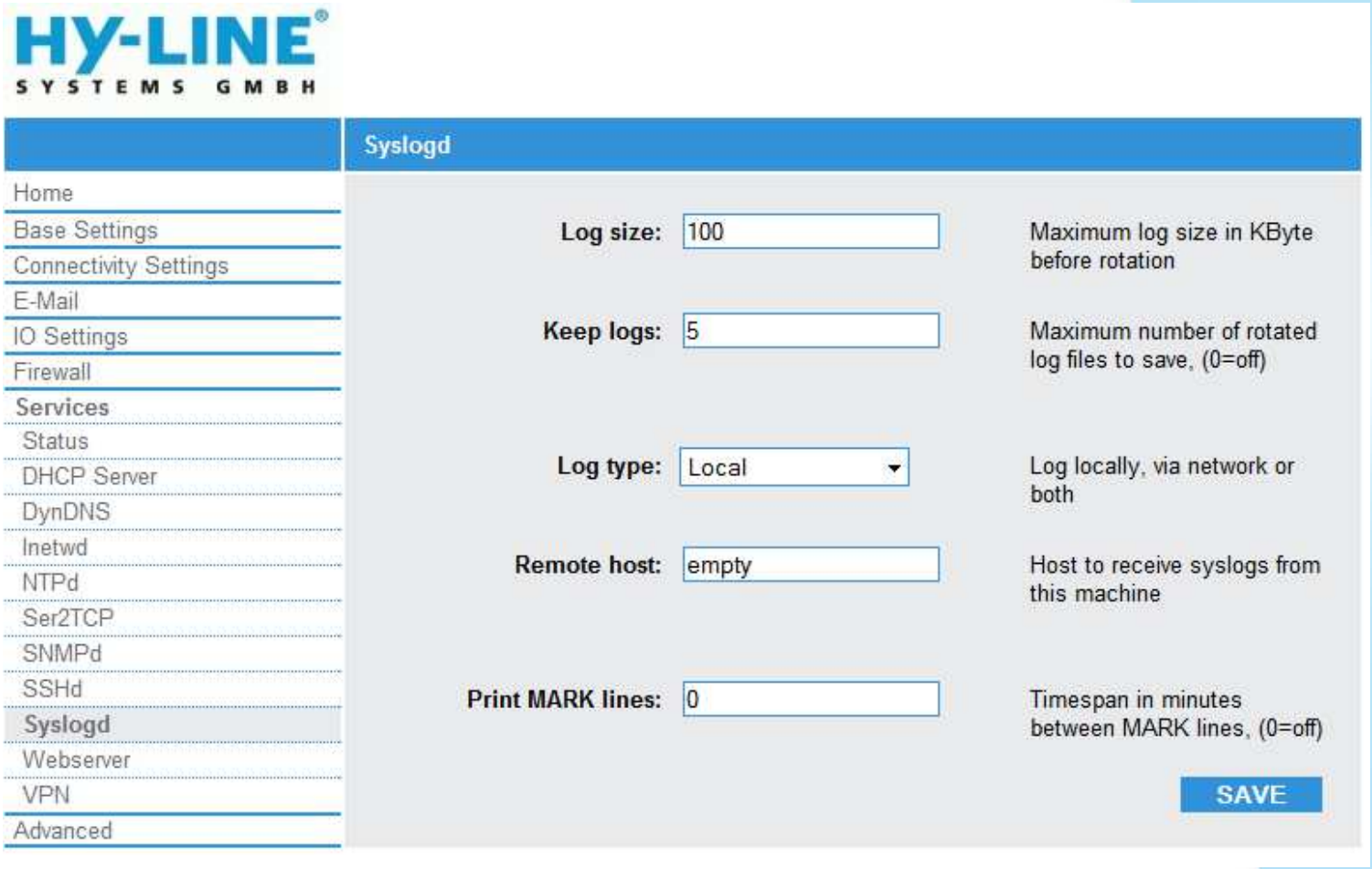
- **Zugang zum Router über SSH-Secure Shell (TCP/IP):**

Windows Programm für den Zugriff: z.B. winscp

login: *root* **passwort:** *changemetoo* Änderbar unter User Management (root ist ein System user)
Einstellung SSH (TCP/IP): Host-Name oder IP-Addresse: *Router-IP* Port: *22*

Info: **Die erste Initialisierung des SSH-Keys erfolgt nach einem Firmware Update (oder im Auslieferungszustand). Dafür muss der Router für ca. 15 Minuten eingeschaltet sein. Danach ist der Router per SSH erreichbar!**

Services - Syslogd:



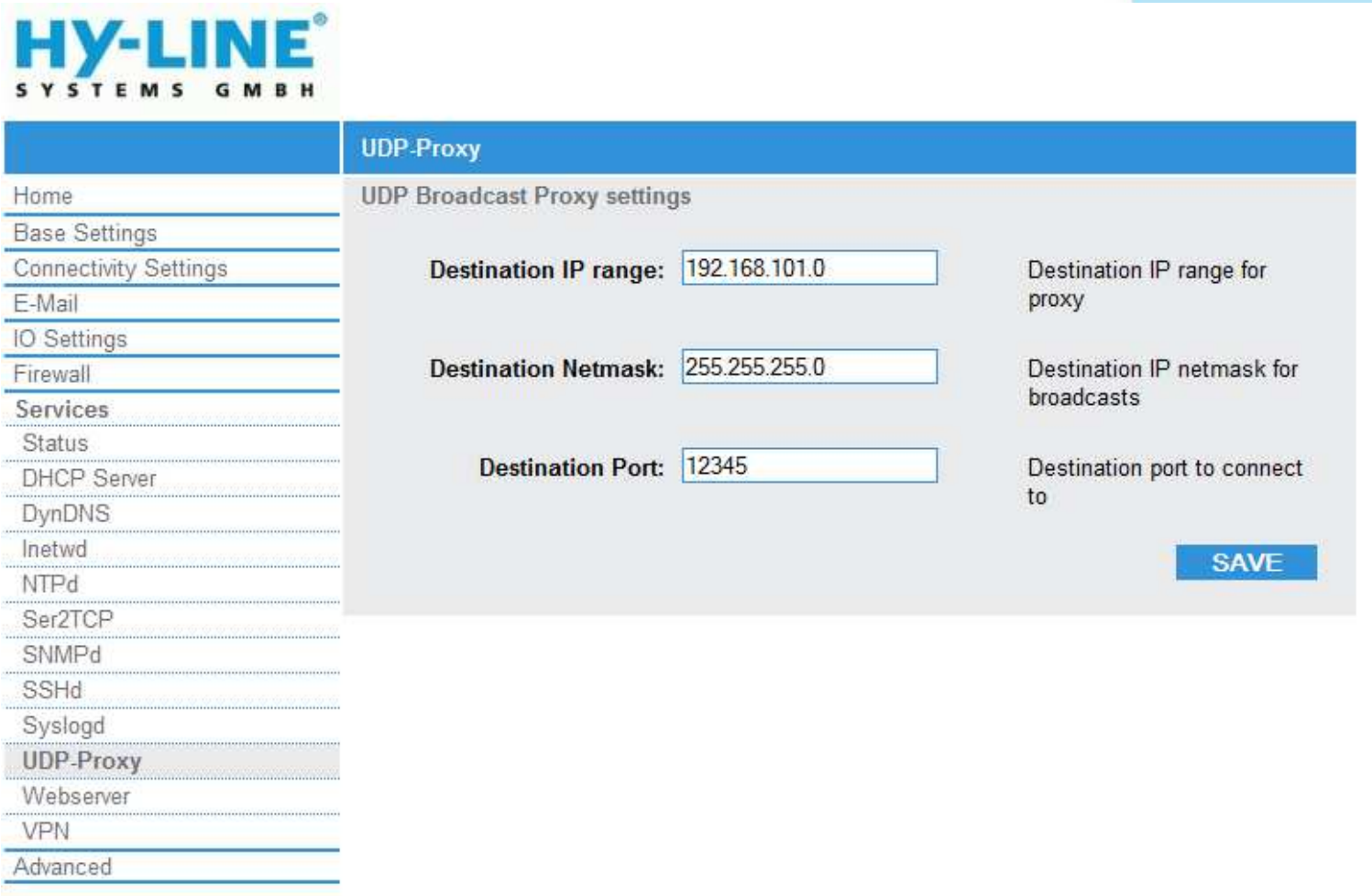
Menü zum Einstellen der Logfile Größe, Anzahl de Logfiles und Remote Loggings.

Services - FTP-Server:

Benutzername: root
Passwort: changemetoo

- ca. 3MB Flash-Speicher (persistent, im root Verzeichnis)
- ca. 8MB RAM-Speicher (in Unterverzeichnis von ..\tmp)

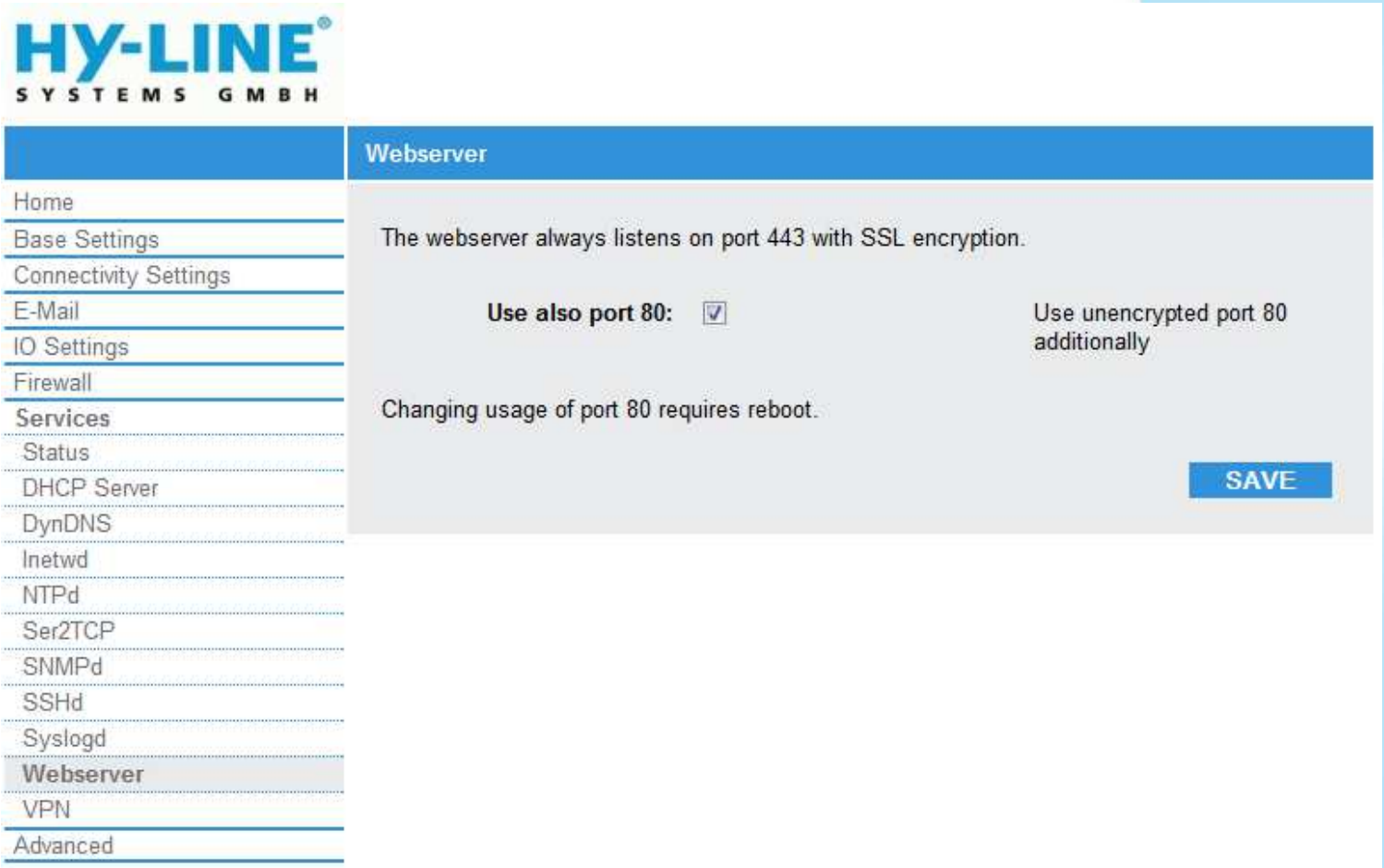
Services - UDP Broadcast Proxy:



Die UDP-Broadcast Funktion dient zum automatischen finden von Netzwerkgeräten im HY-LINE Router Subnetz (Discover Funktion). Hierzu wird ein aus dem Internet kommendes UDP-Paket an den HY-LINE Router anhand des Ports identifiziert. Ist der Port im UDP-Paket der angegebene Destination Port (siehe oben), dann wird ein Broadcast des UDP Paketes ins angegebene IP Subnetz des Routers gesendet. Alle Antworten werden dann zurück an den Absender geschickt.

- **Destination IP range:** Ziel IP-Bereich, in das der Broadcast geschickt wird (im Standard der IP Bereich der LAN-Schnittstelle des Routers)
- **Destination Netmask:** Ziel Subnetz, in das der Broadcast geschickt wird
- **Destination Port:** Identifizierung des eingehenden UDP-Pakets und Zielportadresse der Geräte im Router Netz

Services - Webserver:



Use also Port 80 aktiviert: der Router ist erreichbar unter http mit Port 80 und unter https mit Port 443

Hinweis: aus Sicherheitsgründen wird empfohlen, die Verwendung des Port 80 zu deaktivieren.

HTTPS-Zertifikatswarnung: beim Aufruf des Routers über https erscheint eine Zertifikatswarnung, da im HY-LINE Router im Auslieferzustand ein allgemein gültiges Zertifikat installiert ist. Es können eigene, durch eine Zertifizierungsstelle zertifizierte Zertifakte, kundenseitig eingespielt werden.

VPN:

Ein **Virtual Private Network** (**VPN**) (deutsch: Virtuelles Privates Netzwerk) ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netz (zum Beispiel das Internet) nutzt. Teilnehmer eines VPN können Daten wie in einem internen LAN austauschen. Die einzelnen Teilnehmer selbst müssen hierzu nicht direkt verbunden sein. Die Verbindung über das öffentliche Netz wird üblicherweise verschlüsselt. Der Begriff "Private" impliziert jedoch nicht, wie vielfach angenommen, dass es sich um eine verschlüsselte Übertragung handelt. Eine Verbindung der Netze wird über einen Tunnel zwischen VPN-Client und VPN-Server ermöglicht. Meist wird der Tunnel dabei gesichert, aber auch ein ungesicherter Klartexttunnel ist ein VPN.

IP-VPNs nutzen das Internet zum Transport von IP-Paketen unabhängig vom Übertragungsnetz, was im Gegensatz zum direkten Remote-Zugriff auf ein internes Netz (direkte Einwahl beispielsweise über ISDN, GSM...) wesentlich flexibler und kostengünstiger ist.

PPTP-Protokoll:

Das **Point-to-Point Tunneling Protocol** (**PPTP**) ist ein von einem Herstellerkonsortium (Ascend Communications, Microsoft Corporation, 3Com u. a.) entwickeltes Protokoll zum Aufbau eines Virtual Private Network (VPN). Es ermöglicht das Tunneling des PPP durch ein IP-Netzwerk, wobei die einzelnen PPP-Pakete wiederum in GRE-Pakete verpackt werden. Da PPTP in Microsoft Windows integriert ist, ist es trotz einiger Sicherheitsbedenken immer noch sehr verbreitet. Als Kritikpunkt bleibt jedoch immer noch die Tatsache, dass die Verschlüsselungsstärke direkt mit der Länge des eingesetzten Passworts korreliert. PPTP darf bei vernünftig gewählten Passwörtern (zufällige Buchstaben/Zahlenkombinationen) mit einer Mindestlänge von 12 Zeichen als sicher gelten. Daten über PPTP werden in der Regel nur durch höhere Protokolle verschlüsselt, eine Verschlüsselung auf PPTP-Ebene wurde jedoch von Microsoft entwickelt (siehe MPPE). **MPPE** steht für *Microsoft Point*-To-*Point Encryption* Protocol. MPPE soll die Vertrauenswürdigkeit von über PPP übertragenen Paketen sicher stellen. MPPE basiert auf den in RFC 3078 vom März 2001 genannten Verschlüsselungsverfahren.

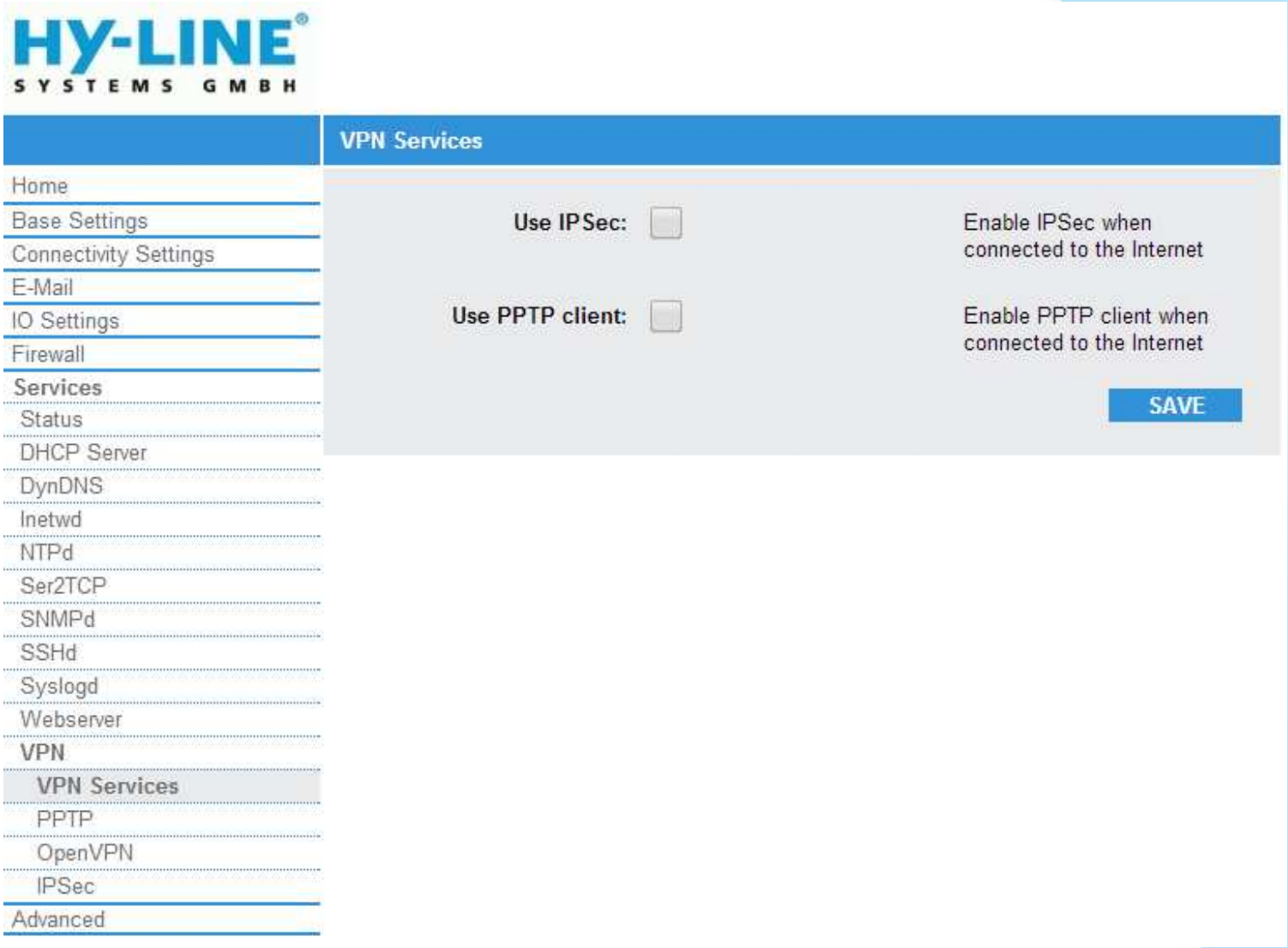
Ipsec-Sicherheitsmechanismus:

IPsec (Kurzform für **IP Security**) wurde 1998 entwickelt, um die Schwächen des Internetprotokolls (IP) zu beheben. Es stellt eine Sicherheitsarchitektur für die Kommunikation über IP-Netzwerke zur Verfügung. IPsec soll die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten. Daneben soll es vor so genannten Replay-Angriffen bzw. einer Replay-Attacke schützen - das heißt, ein Angreifer kann nicht durch Abspielen eines vorher mitgeschnittenen Dialogs die Gegenstelle zu einer wiederholten Aktion verleiten.

IPsec entstand im Zuge der Entwicklung von IPv6 und ist in verschiedenen RFCs spezifiziert: **Sicherheitsarchitektur** für das Internetprotokoll, **Authentication Header, Encapsulating Security Payload,** IPsec **Domain of Interpretation** (IPsec DoI), **Internet Security Association and Key Management Protocol** (ISAKMP), **Internet Key Exchange** (IKE)

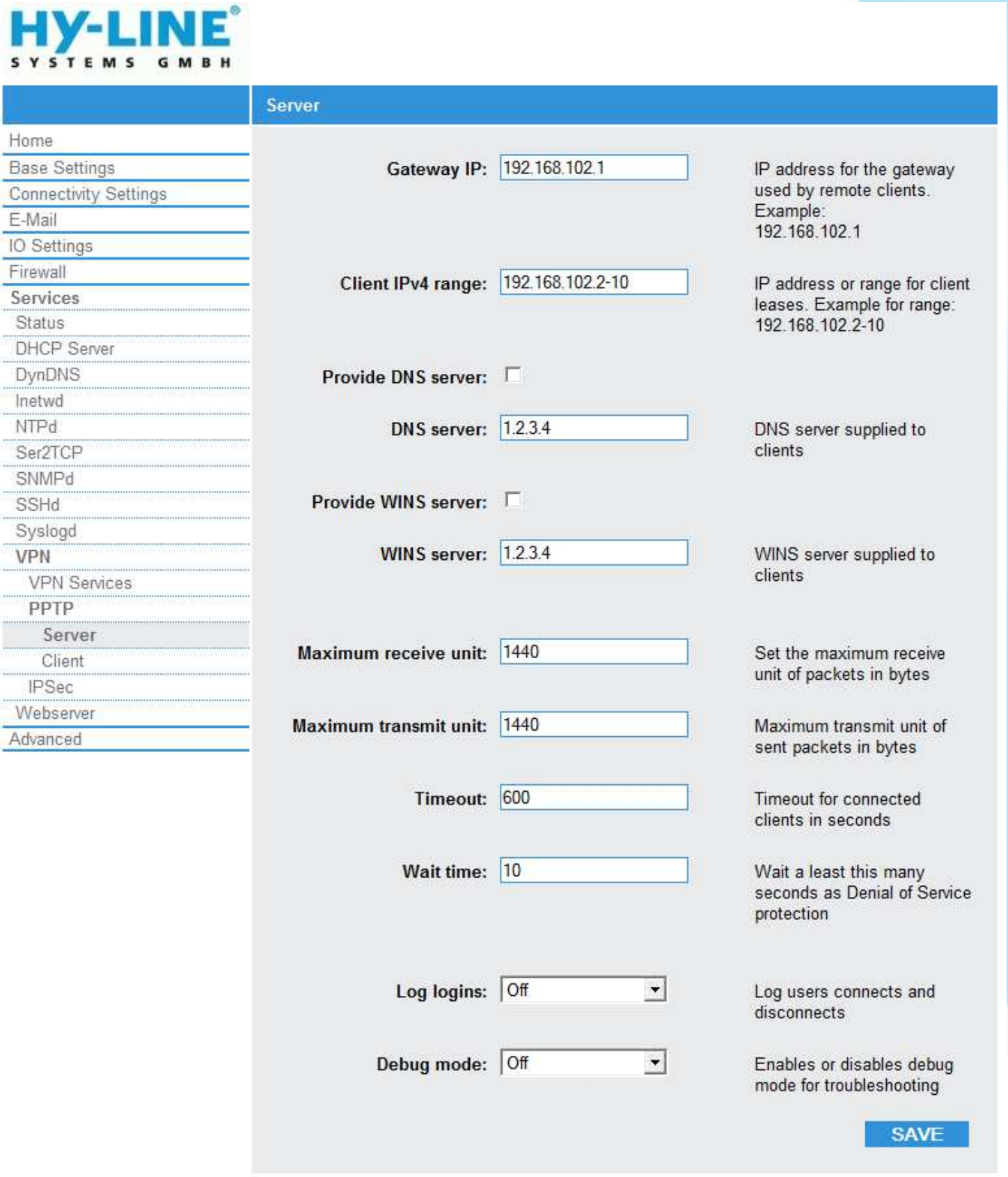
Der RFC 2401 bildet das Hauptdokument zu IPsec, er beschreibt die Architektur von IPsec. Von dort aus werden die oben genannten RFCs referenziert. Wesentliche Inhalte von IPsec sind das *Authentication Header Protokoll (AH)* und das *Encapsulated Security Payload Protokoll (ESP)* sowie das *Internet Key Exchange Protokoll (IKE)* zum Austausch der Schlüssel.Im Gegensatz zu anderen Verschlüsselungsprotokollen wie etwa SSH arbeitet IPsec auf der Netzwerkschicht (Schicht 3) des OSI-Referenzmodells.

Services - VPN



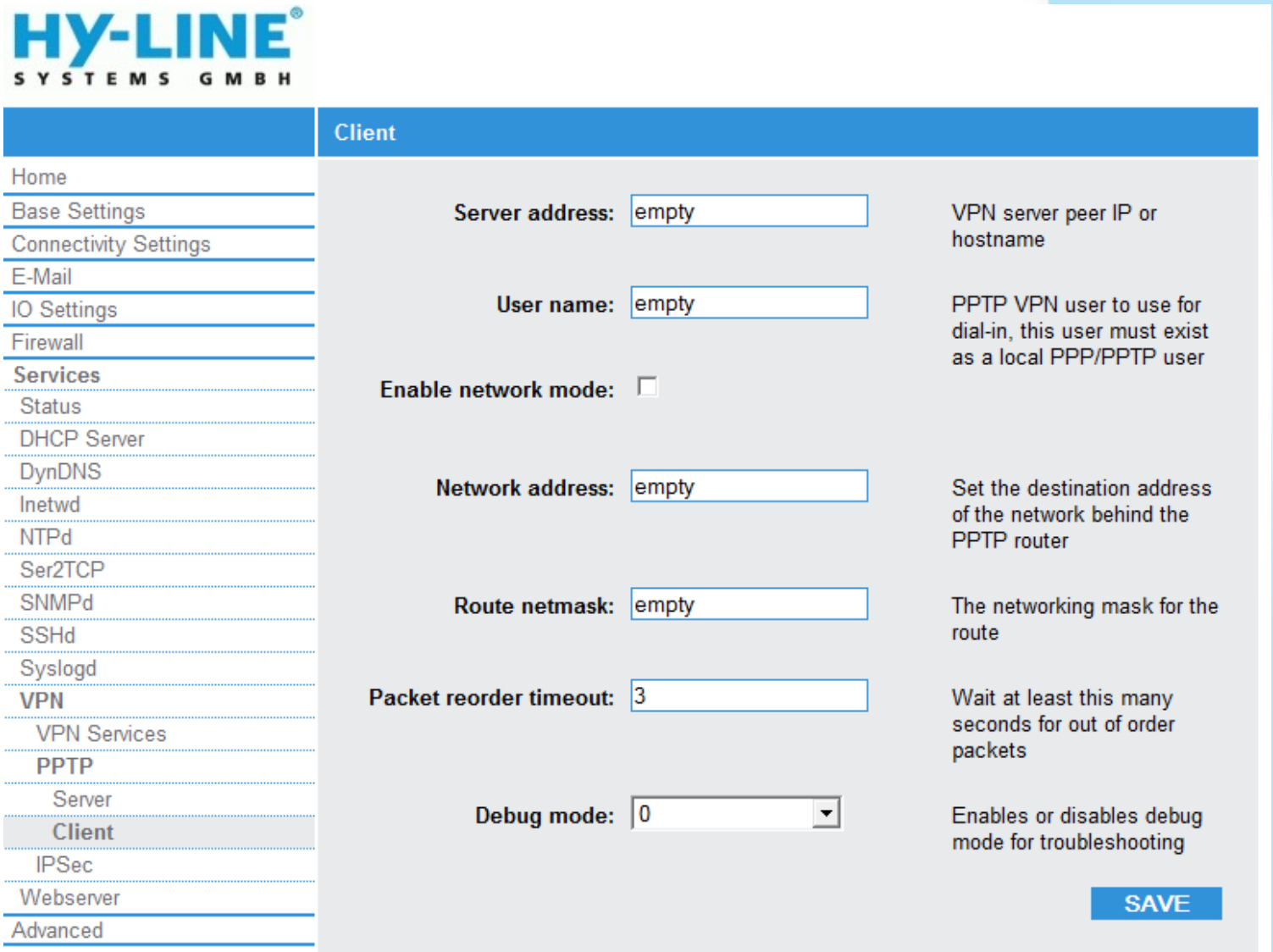
- **Use IPsec:** aktiviert IPsec (Pre-shared key, Zertifikate x.509)
- **Use PPTP server:** aktiviert PPTP Server
- **Use PPTP client:** aktiviert PPTP Client

VPN – PPTP Server Konfiguration:



- **Gateway IP / Client Pv4 range:** Die VPN-Tunnel IP-Subnetze müssen sich vom lokalen Router IP-Subnetz unterscheiden.

VPN – PPTP Client Konfiguration:



- **Server address:** IP-Adresse oder Name des VPN-Servers
- **User name:** Benutzername des VPN-Users (muß im VPN-Server angelegt sein), der Benutzer wird im HY-LINE Router im Benutzermanagement angelegt
- **Enable network mode:** aktiviert das Routing in den VPN-Tunnel (muß im Regelfall aktiviert sein)
- **Network address:** Netzwerk auf der VPN-Server Seite, Syntax: xxx.xxx.xxx.**0**
- **Route netmask:** Subnetz für die Route, Syntax: 255.255.255.**0**
- **Route manuell setzen auf linux shell:** -sys sh -ip route add 192.168.3.0/24 add ppp1

VPN-PPTP Verbindungen erstellen & verwalten

- Der HY-LINE M2M Router wurde mit dem Router der Firma Funkwerk, Typ Bintek R1200/3000, auf einwandfreie Funktion im VPN-PPTP Verbindungsmodus getestet (M2M-Router: VPN-Client, Bintek Router: VPN-Server).

- Die folgenden Einstellungen müssen im M2M Router vorgenommen werden. Zu beachten ist das die Einstellungen mit der aktuellen Firmware nicht über die Web-Oberfläche vorgenommen werden können. Diese können über die serielle Schnittstelle mittels eines Terminal Programms (Hyper Terminal) oder über eine SSH-Verbindung (z.B. Putty, oder besser WinSCP) durchgeführt werden.

M2M Router Einstellung für den Betrieb als VPN-PPTP-CLIENT:

- **Benutzerauthentifizierung einstellen**:
  - Der Router unterstützt CHAP und MS-CHAP V2. Die Authentifizierung muß fest auf einen Wert eingestellt werden. Folgende Datei dazu edititeren: \\etc\runit\pptp\run (Datei mit der Endung script wählen, nicht mit Endung template)

    - **CHAP:** `name +mppe-40 persist maxfail 0 debug \`
      -> M2M Router versucht zuerst Chap, dann MS-CHAP V2 zu authentifizieren

    - **MS-Chap V2**: `name +mppe-40 refuse-chap persist maxfail 0 debug \`
      -> M2M Router ist fest auf MS-CHAP V2 eingestellt

- **Verschlüsselung einstellen (MPPE):**
  - Der Router unterstützt die Verschlüsselung nach MPPE mit 40Bit und 128Bit oder MPPE ausgeschaltet für MS-CHAP V2 (Chap unterstützt keine Verschlüsselung). Die Verschlüsselung muß fest auf einen Wert eingestellt werden. Folgende Datei dazu edititeren: \\etc\runit\pptp\run (Datei mit der Endung script wählen, nicht mit Endung template) Stringbeispiele siehe Punkt Benutzerauthentifizierung.

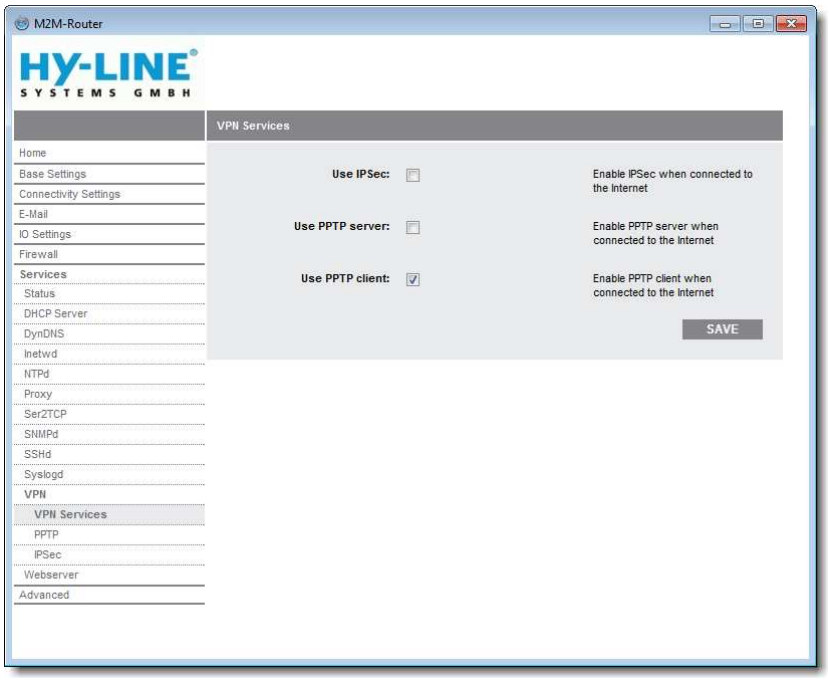
    - +mppe-40
    - +mppe-128
    - Ausschalten: kompletten String (+mppe-40 oder +mppe-128) weglassen

Empfohlene Einstellung des M2M Routers in Verbindung mit dem Bintec R1200/3000:

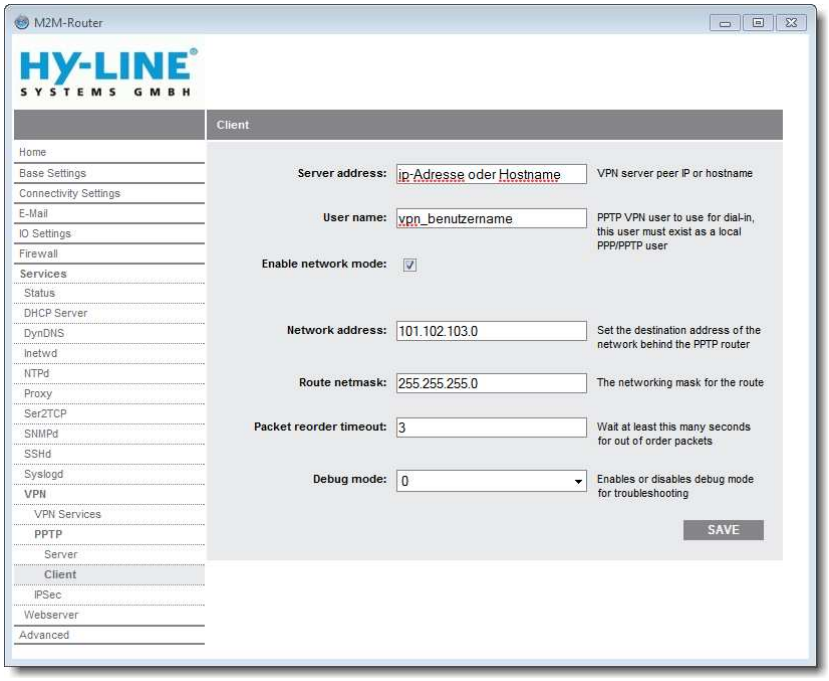
- M2M Router fest eingestellt auf MS-CHAP V2 und auf MPPE mit 128Bit
  - `name +mppe-128 refuse-chap persist maxfail 0 debug \`

- Bintek R1200/3000 fest eingestellt auf MS-CHAP V2 und MPPE 128Bit (Standard, V2 oder RFC 3078)

Folgende Einstellungen auf der M2M Router Webseite einstellen:



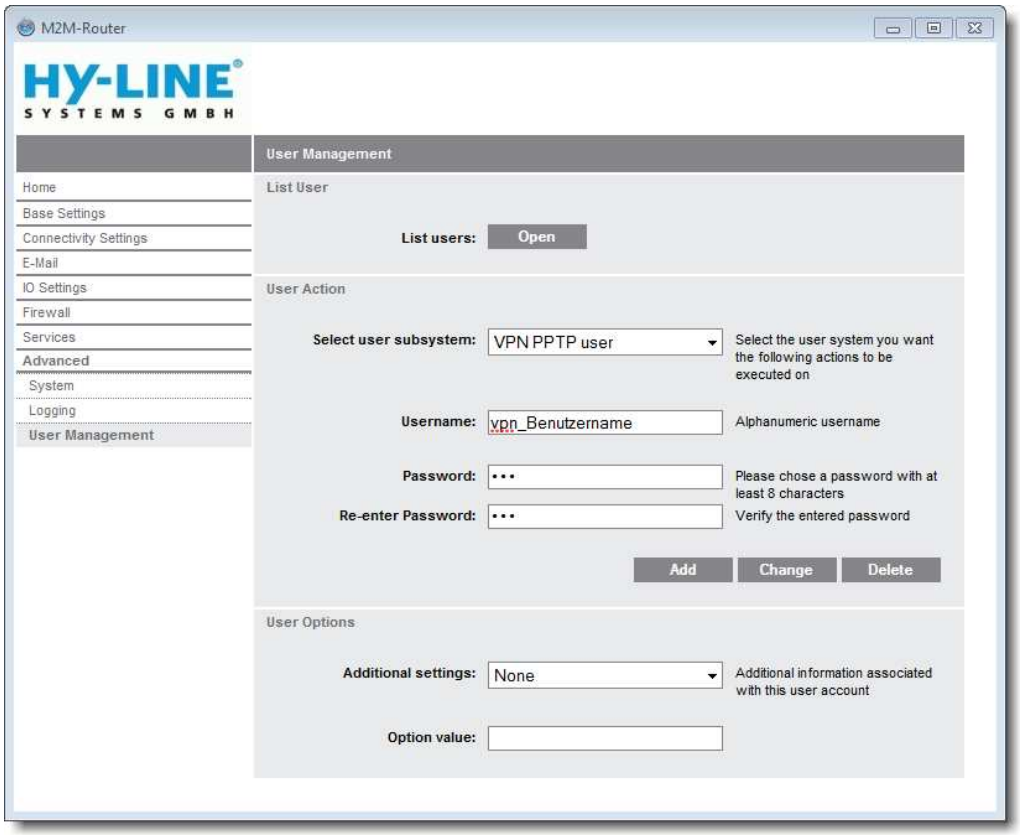
- **VPN Services:** *Use PPTP client* aktivieren



- **VPN \ PPTP \ Client :**
  - VPN Server eintragen
  - Benutzername eintragen, diesen Benutzer auf M2M Router anlegen, siehe nächste Seite in diesem Handbuch
  - Network Mode einschalten, dadurch wird das Routing aktiviert (Gateway (M2M Router IP) in die Geräte eintragen, die sich im M2M Router Netz befinden)
  - Network address: hier den Adressbereich hinter dem VPN Router (Server) angeben, Format: IP Adresse mit 4. Ziffer als 0
  - Alle anderen Einstellungen wie im Bild oben

Benutzermanagement: VPN-PPTP Benutzer anlegen

- **Benutzer anlegen über Weboberfläche unter Advanced\ User Management**:
  - Benutzer als Typ: PPP/PPTP User anlegen



Wichtig: nach dem Anlegen neuer Benutzer muß eine Datei editiert werden, damit die Benutzereinstellungen kompatibel zum Bintek Router gespeichert sind

- **Editieren und speichern der Datei:** \etc\ppp\chap-secrets
- Eintrag von ***username PPP password*** ändern in ***username * password ****

```
# PPP
t-d1 * t-d1
# PPTP
vpn ppp 123 *
# PPTP
username ppp password *
```

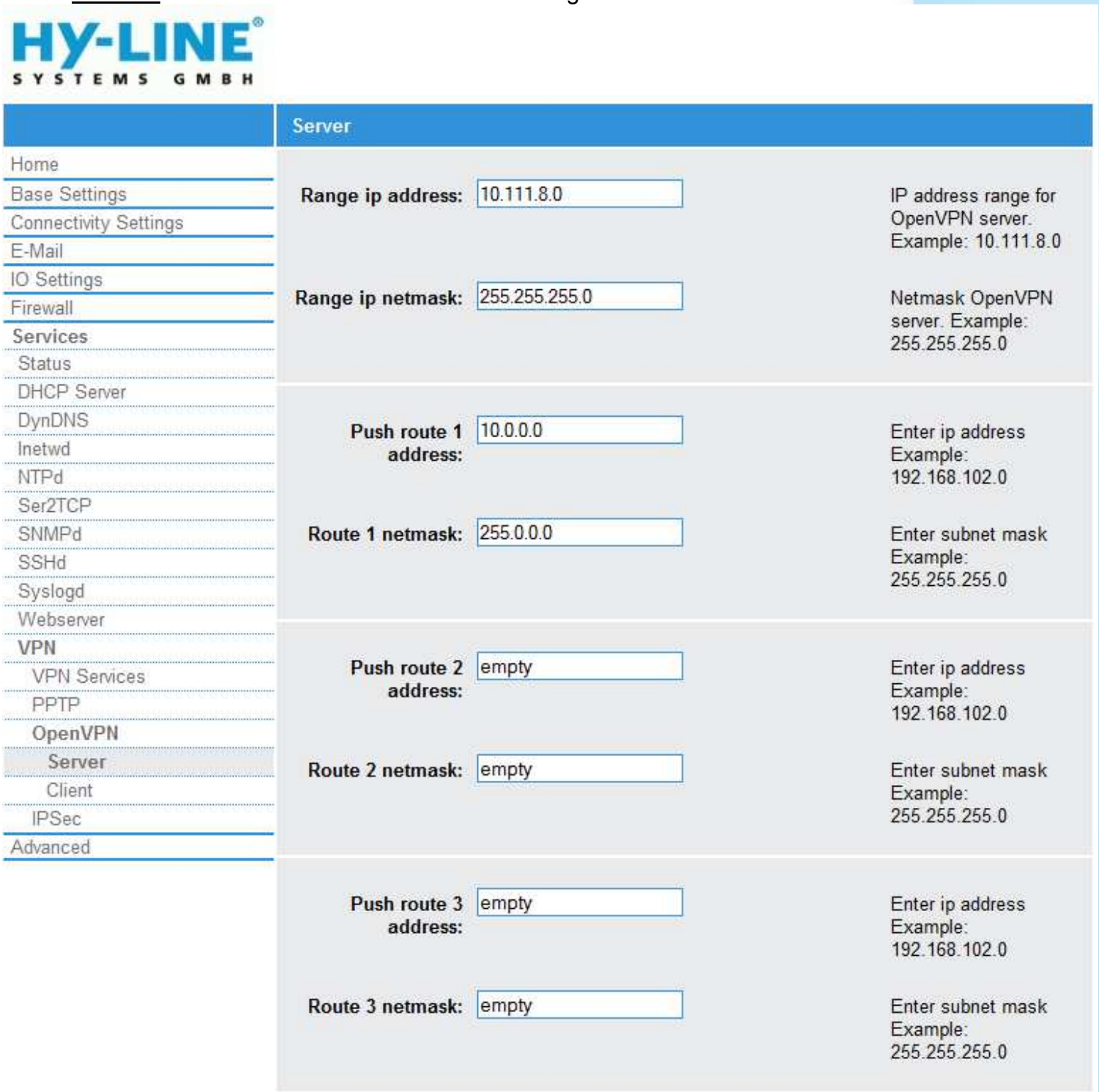
ändern in

```
username * password *
```

Wichtig: diese Änderung muß jedesmal neu gemacht werden, wenn Benutzer neu angelegt oder geändert werden!

VPN – OpenVPN Server Konfiguration:

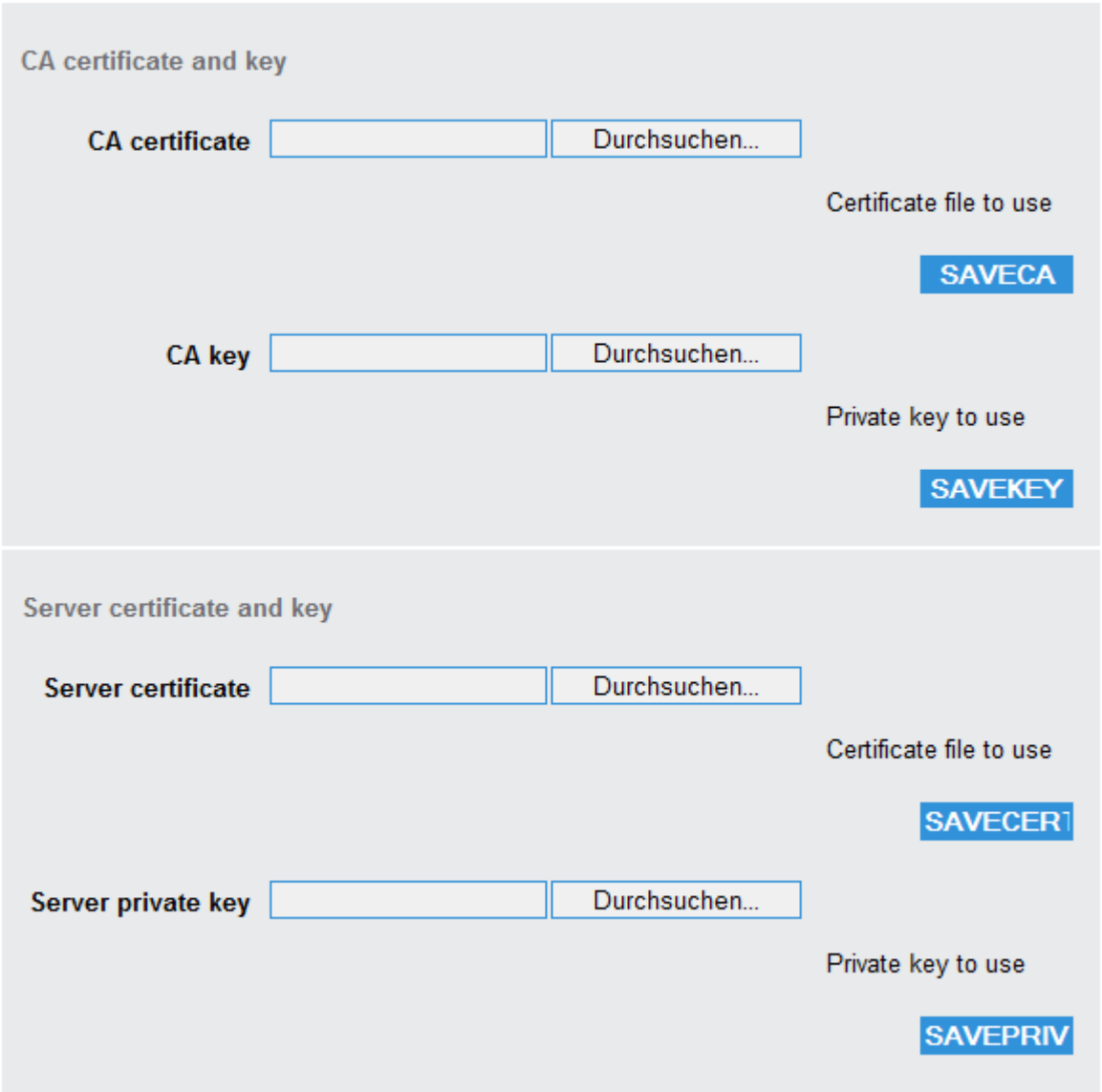
- **OpenVPN Server Konfiguration:**
  Hinweis: die interne Router Uhr muß korrekt eingestellt sein



- **Range ip Address:** IP-Adressbereich des aufgebauten OpenVPN Tunnels (Format: x.x.x.0)
- **Range ip netmask:** IP-Netzmaske des aufgebauten OpenVPN Tunnels
- **Push route 1-3:** IP-Adressbereich, wird als Route im OpenVPN Client gesetzt (Format: x.x.x.0)
- **Route 1-3 netmask:** IP-Subnetz, wird als Subnetz der Route im OpenVPN Client gesetzt

VPN – OpenVPN Server Konfiguration:

- **Duplicate cn:** ermöglicht mehreren Clients, die denselben Common name haben, sich gleichzeitig mit dem Router zu verbinden



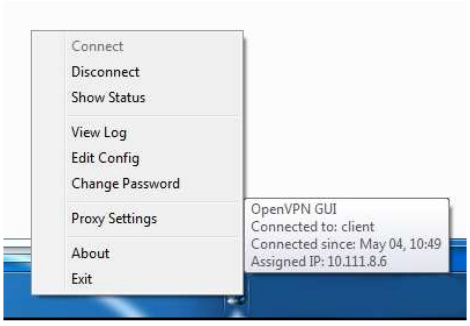
- **Authentifizierung:** die Authentifizierung erfolgt im HY-LINE Router ausschließlich durch Zertifikate. Standardzertifikate können Sie beim HY-LINE Support anfragen.
- **Verschlüsselung:** SHA1 als HMAC und BF-CBC (Blowfish im Cyper-Block-Chaining Mode) Die Default-Keysize ist bei SHA1 160 bit und bei BF-CBC 128 bit. (nicht konfigurierbar)
- **OpenVPN Client:** unter Windows kann folgender Client verwendet werden:

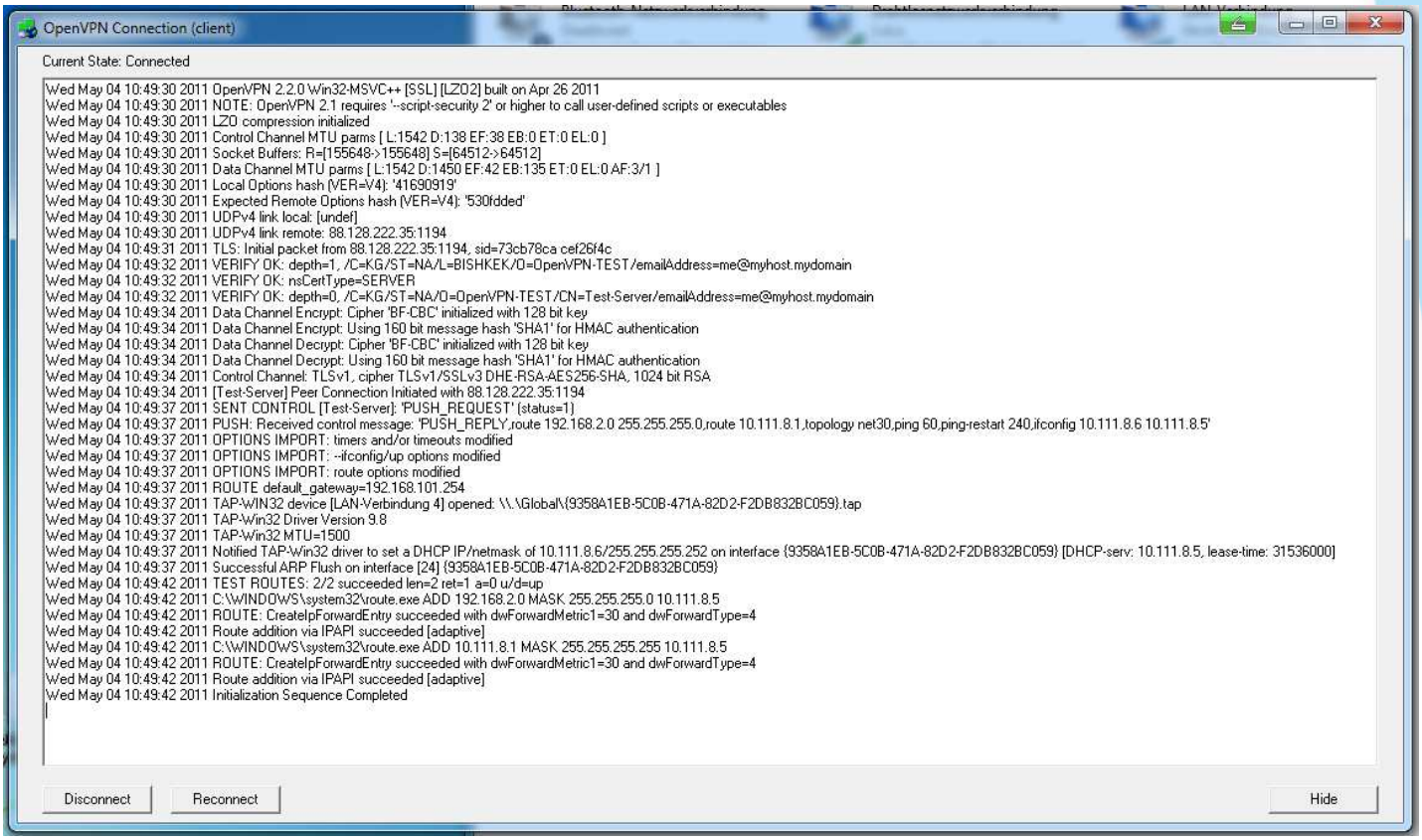
http://openvpn.net/index.php/open-source/downloads.html

VPN – OpenVPN Server Konfiguration:

- **OpenVPN Client Konfiguration auf der Gegenseite (z.B.PC-System / Hardware-Router):**
  - Zertifikate + Keys in HY-LINE Router einspielen, OpenVPN Namen der Zertifikate und Keys müssen dieses Format haben:
    > ca.crt
    > ca.key
    > client.crt
    > client.key
    > server.crt
    > server.key
  - Zertifikate + Keys auf dem PC in die entsprechenden Verzeichnisse kopieren (z.B. ..\Programme\OpenVPN\Config
  - OpenVPN Client Software Config File anpassen (z.B. client.ovpn)

- **Folgendes Bild und Log zeigt einen erfolgreichen OpenVPN Tunnel zum HY-LINE Router (VPN-Server) von einem PC mit Windows 7:**

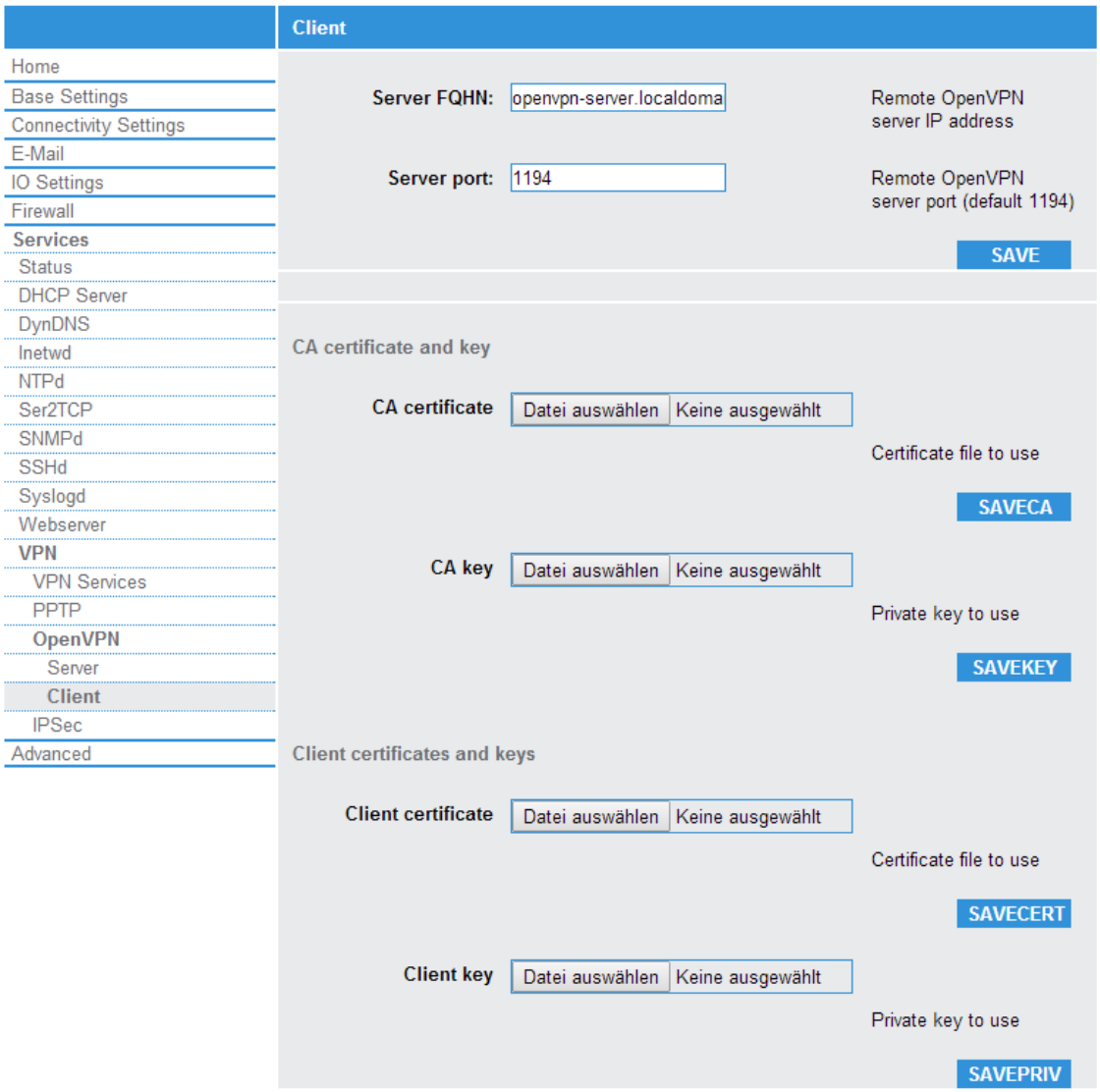



OpenVPN Connection (client)
Current State: Connected
Wed May 04 10:49:30 2011 OpenVPN 2.2.0 Win32-MSVC++ [SSL] [LZO2] built on Apr 26 2011
Wed May 04 10:49:30 2011 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or executables
Wed May 04 10:49:30 2011 LZO compression initialized
Wed May 04 10:49:30 2011 Control Channel MTU parms [L:1542 D:138 EF:38 EB:0 ET:0 EL:0]
Wed May 04 10:49:30 2011 Socket Buffers: R=[155648->155648] S=[64512->64512]
Wed May 04 10:49:30 2011 Data Channel MTU parms [L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1]
Wed May 04 10:49:30 2011 Local Options hash (VER=V4): '41690919'
Wed May 04 10:49:30 2011 Expected Remote Options hash (VER=V4): '530fdded'
Wed May 04 10:49:30 2011 UDPv4 link local: [undef]
Wed May 04 10:49:30 2011 UDPv4 link remote: 88.128.222.35:1194
Wed May 04 10:49:31 2011 TLS: Initial packet from 88.128.222.35:1194, sid=73cb78ca cef26f4c
Wed May 04 10:49:32 2011 VERIFY OK: depth=1, /C=KG/ST=NA/L=BISHKEK/O=OpenVPN-TEST/emailAddress=me@myhost.mydomain
Wed May 04 10:49:32 2011 VERIFY OK: nsCertType=SERVER
Wed May 04 10:49:32 2011 VERIFY OK: depth=0, /C=KG/ST=NA/O=OpenVPN-TEST/CN=Test-Server/emailAddress=me@myhost.mydomain
Wed May 04 10:49:34 2011 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed May 04 10:49:34 2011 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed May 04 10:49:34 2011 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed May 04 10:49:34 2011 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed May 04 10:49:34 2011 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Wed May 04 10:49:34 2011 [Test-Server] Peer Connection Initiated with 88.128.222.35:1194
Wed May 04 10:49:37 2011 SENT CONTROL [Test-Server]: 'PUSH_REQUEST' (status=1)
Wed May 04 10:49:37 2011 PUSH: Received control message: 'PUSH_REPLY,route 192.168.2.0 255.255.255.0,route 10.111.8.1,topology net30,ping 60,ping-restart 240,ifconfig 10.111.8.6 10.111.8.5'
Wed May 04 10:49:37 2011 OPTIONS IMPORT: timers and/or timeouts modified
Wed May 04 10:49:37 2011 OPTIONS IMPORT: --ifconfig/up options modified
Wed May 04 10:49:37 2011 OPTIONS IMPORT: route options modified
Wed May 04 10:49:37 2011 ROUTE default_gateway=192.168.101.254
Wed May 04 10:49:37 2011 TAP-WIN32 device [LAN-Verbindung 4] opened: \\.\Global\{9358A1EB-5C0B-471A-82D2-F2DB832BC059}.tap
Wed May 04 10:49:37 2011 TAP-Win32 Driver Version 9.8
Wed May 04 10:49:37 2011 TAP-Win32 MTU=1500
Wed May 04 10:49:37 2011 Notified TAP-Win32 driver to set a DHCP IP/netmask of 10.111.8.6/255.255.255.252 on interface {9358A1EB-5C0B-471A-82D2-F2DB832BC059} [DHCP-serv: 10.111.8.5, lease-time: 31536000]
Wed May 04 10:49:37 2011 Successful ARP Flush on interface [24] {9358A1EB-5C0B-471A-82D2-F2DB832BC059}
Wed May 04 10:49:42 2011 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Wed May 04 10:49:42 2011 C:\WINDOWS\system32\route.exe ADD 192.168.2.0 MASK 255.255.255.0 10.111.8.5
Wed May 04 10:49:42 2011 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=30 and dwForwardType=4
Wed May 04 10:49:42 2011 Route addition via IPAPI succeeded [adaptive]
Wed May 04 10:49:42 2011 C:\WINDOWS\system32\route.exe ADD 10.111.8.1 MASK 255.255.255.255 10.111.8.5
Wed May 04 10:49:42 2011 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=30 and dwForwardType=4
Wed May 04 10:49:42 2011 Route addition via IPAPI succeeded [adaptive]
Wed May 04 10:49:42 2011 Initialization Sequence Completed
Disconnect
Reconnect
Hide

VPN – OpenVPN Client Konfiguration:

- **OpenVPN Client Konfiguration:**
  Hinweis: die interne Router Uhr muß korrekt eingestellt sein

- **Akivieren des OpenVPN Client über das Service Menü:**



- **Server FQHN:** openVPN Server IP-Adresse oder Domain-Name
- **Server port:** openVPN Server Port
- **Client certificate:** Zertifikat zur Authentifizierung
- **Client key:** Key zur Authentifizierung
- **CA certificate:** CA-Zertifikat zur Authentifizierung, wird im OpenVPN SERVER Menü eingetragen
- **CA key:** CA-Key zur Authentifizierung, wird im OpenVPN SERVER Menü eingetragen

VPN –IPsec Server Konfiguration:

VPN-ipsec Preshared Key Verbindungen erstellen & verwalten

Netzwerk Beispielkonfiguration:

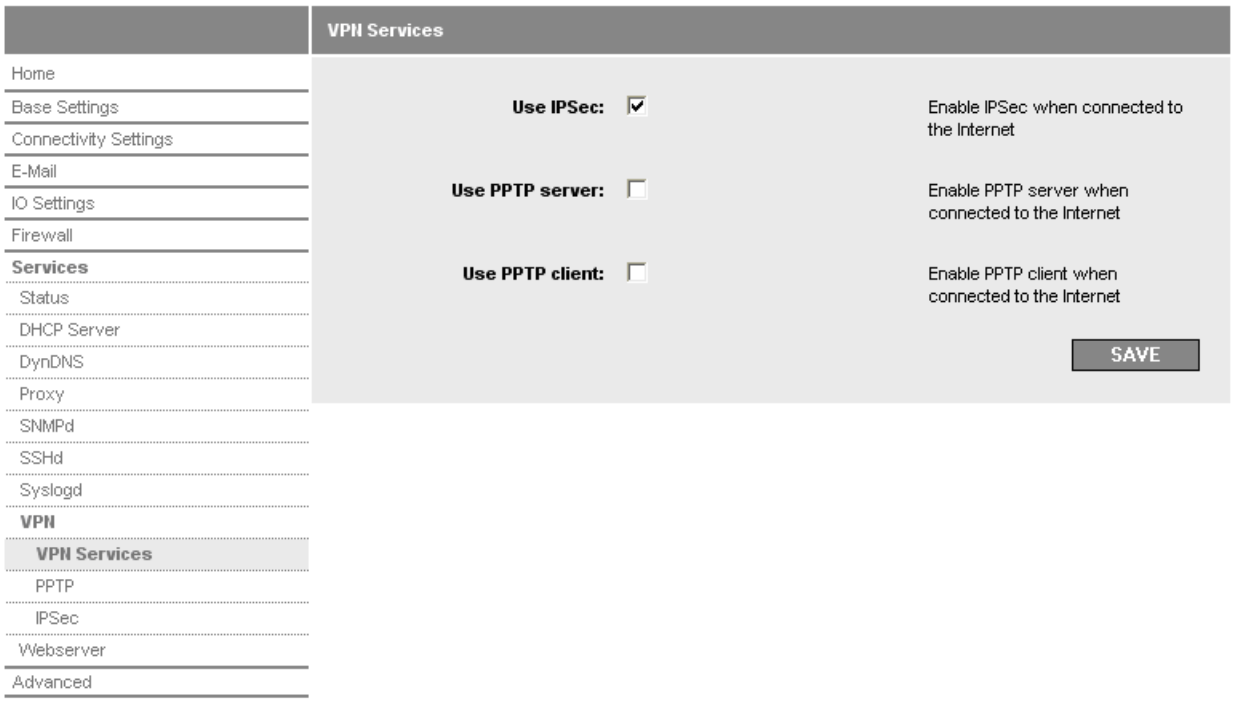
RECHENZENTRUM
Router-IP WAN: 201.202.203.204
Netz : 192.168.180.0/24 255.255.255.0

Remote Netz (HY-LINE Router)
Router-IP WAN: dynamisch
Router-IP LAN: 192.168.3.254
Netz : 192.168.3.0/24 255.255.255.0

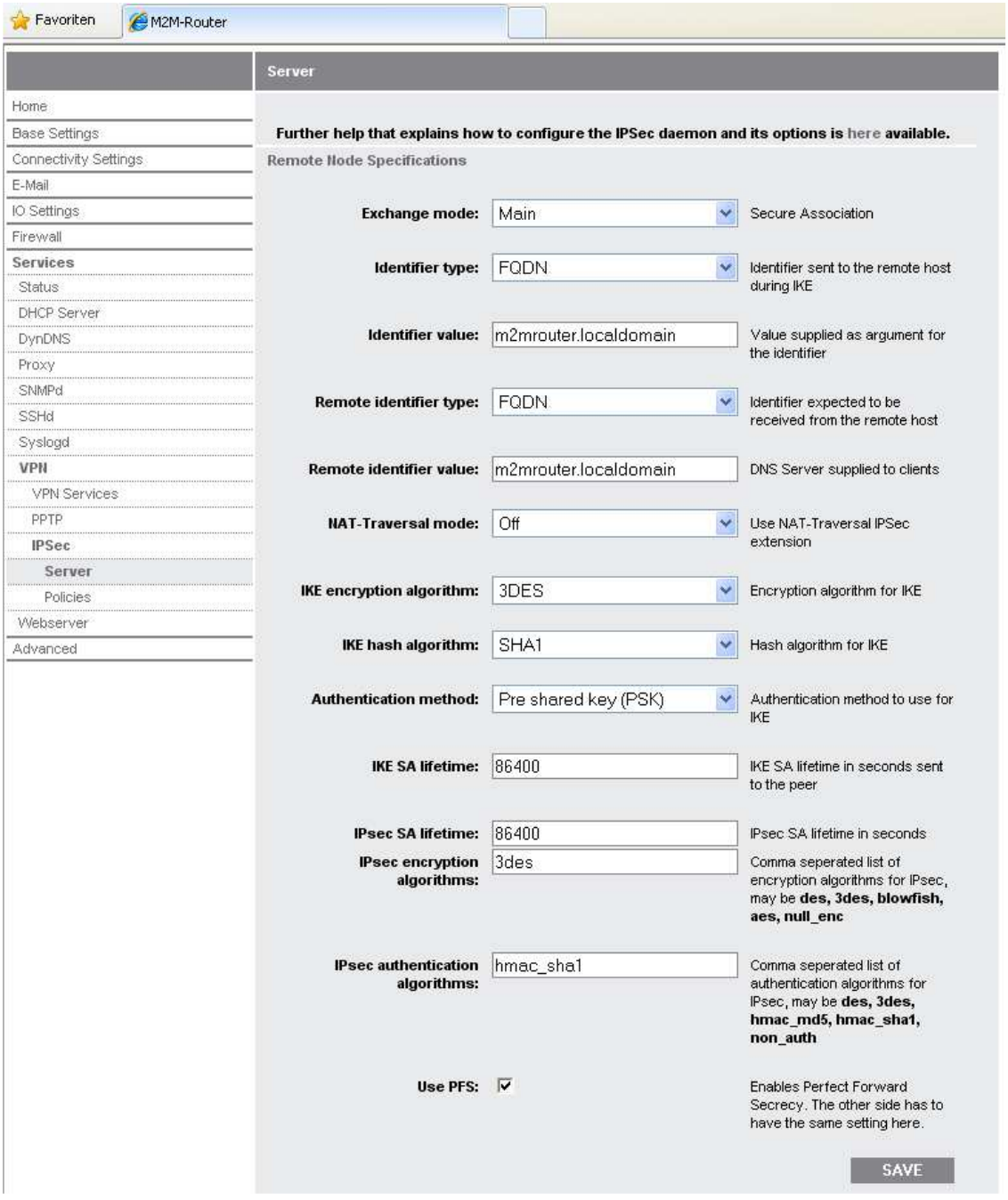
ipsec PHASE 1 PARAMETER (management connection)
Verschlüsselung (Encryption) : 3DES
Authentifizierung (Hash) : SHA1
Preshared Key : 12345
Lifetime : 86400

ipsec PHASE 2 PARAMETER (data connection)
Sicherheits-Protokoll : ESP (nicht AH)
Conection Mode : Tunnel Mode (nicht Transport Mode)
Verschlüsselung (Encryption) : 3DES
Authentifizierung (Hash) : SHA1
Perfect Forward Secrecy (pfs-Group) : 2 (enabled) – DH2: Diffie Hellmann Group 2

ipsec aktivieren:



ipsec konfigurieren:



Hinweise:

- nicht benötigte Werte (z.B. identifier value, type, etc) auf Standard-Einstellung belassen
- ipsec Algorithmen (encryption/authentication) per Hand eintragen, Syntax beachten

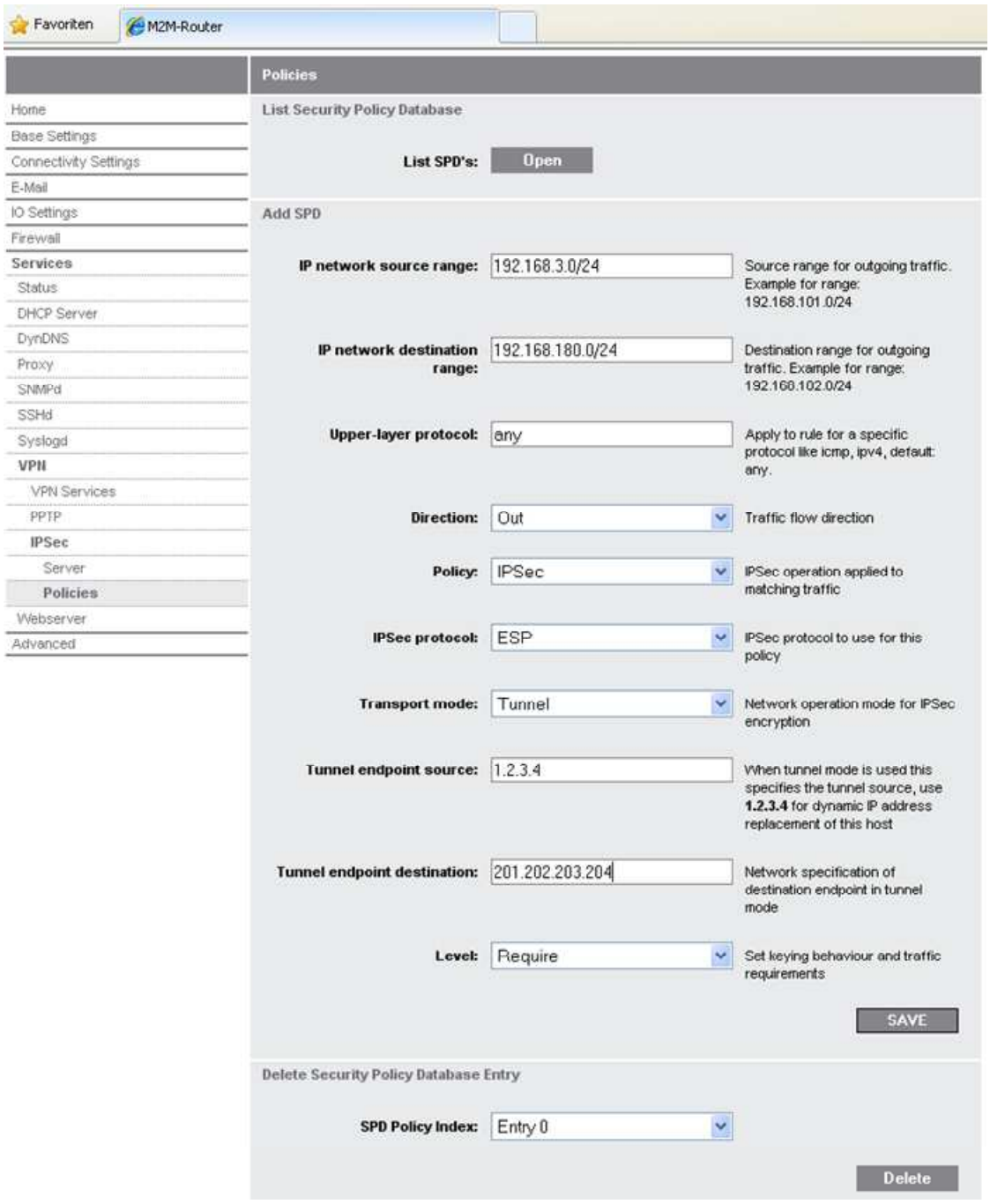
ipsec Policies (Routing):

RECHENZENTRUM
Router-IP WAN: 201.202.203.204
Netz : 192.168.180.0/24
255.255.255.0

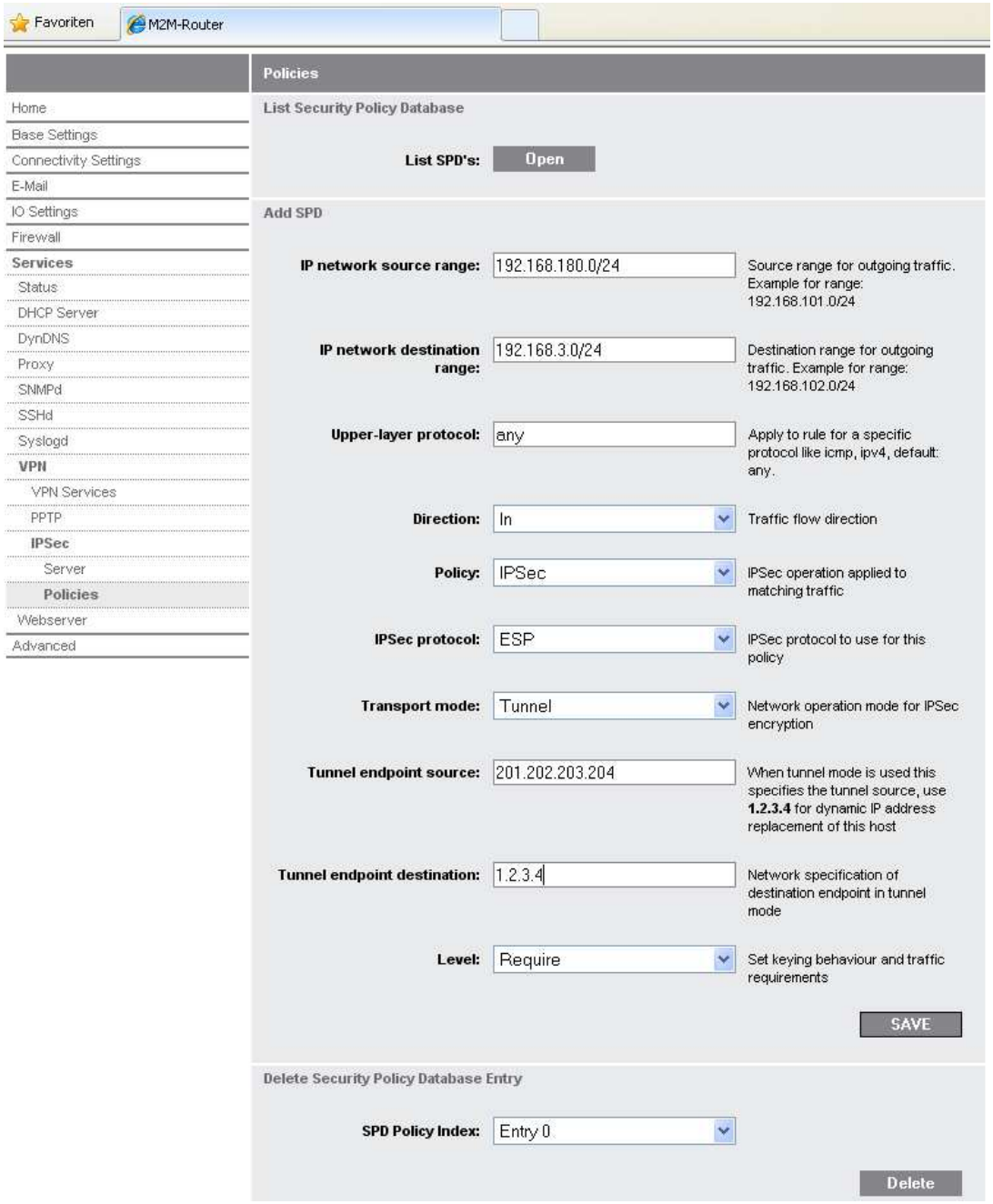
Remote Netz (HY-LINE Router)
Router-IP WAN: dynamisch
Router-IP LAN: 192.168.3.254
Netz : 192.168.3.0/24
255.255.255.0

Hier müssen im HY-LINE Router 2 Routen konfiguriert werden, eine für ausgehenden Traffic (out) und eine für eingehenden Traffic (in).

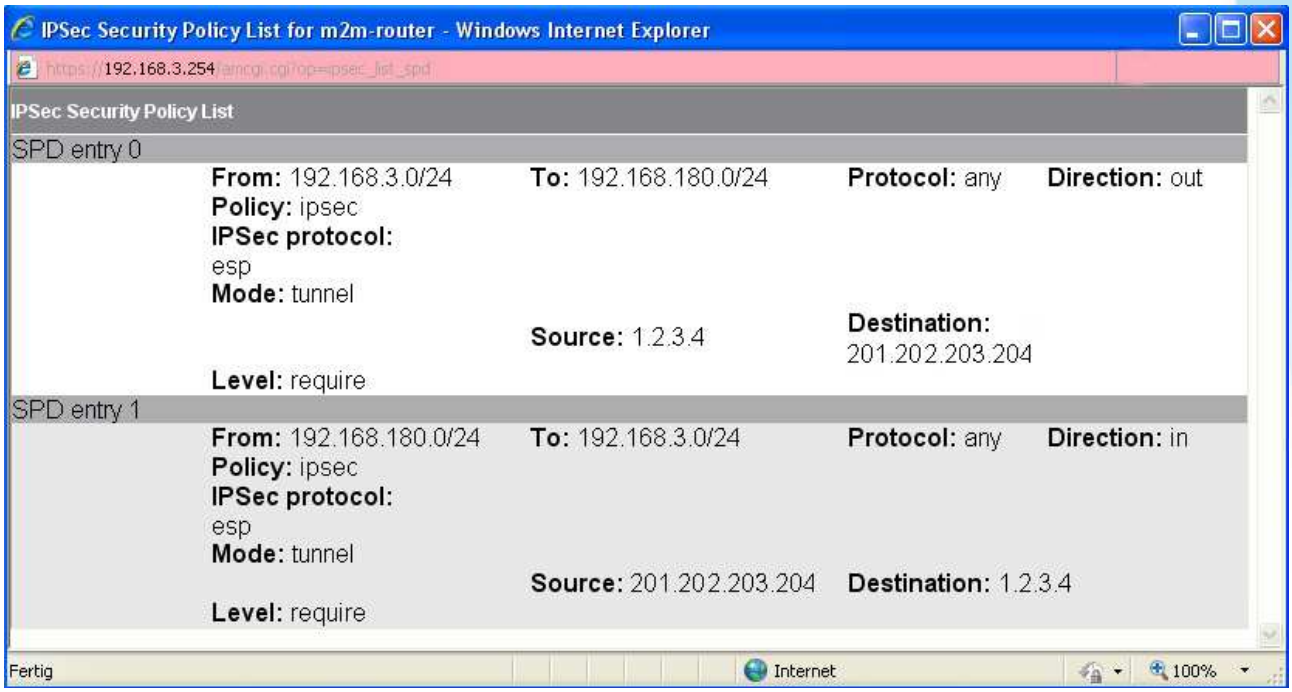
ipsec Policies OUT:



ipsec Policies IN:



ipsec Policies Übersicht:



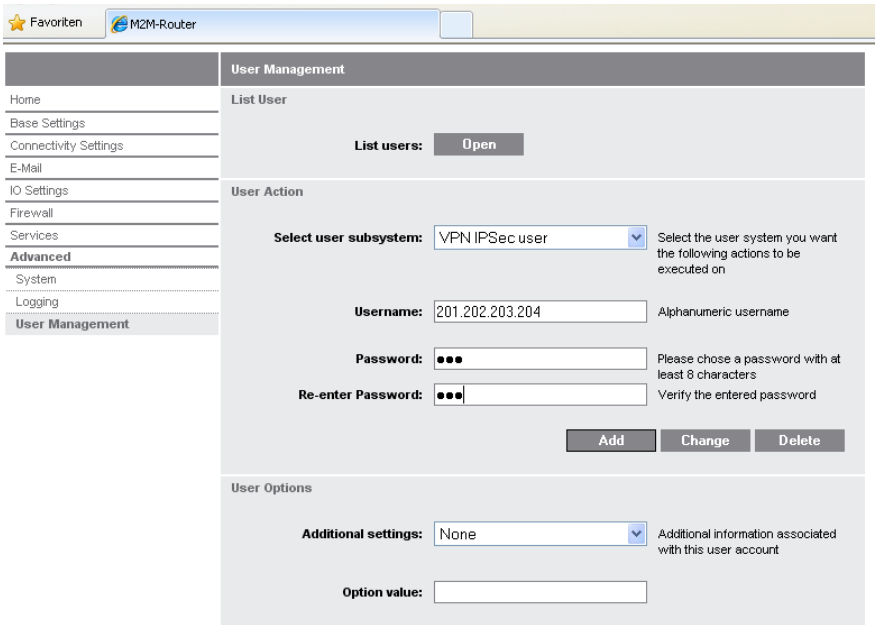
Benutzer anlegen:

Im Menü \Advanced\User Management wird nun ein Benutzer angelegt wie folgt:

User subsystem: VPN ipsec user

Username: öffentliche WAN-IP der Gegenstelle (hier Rechenzentrum)

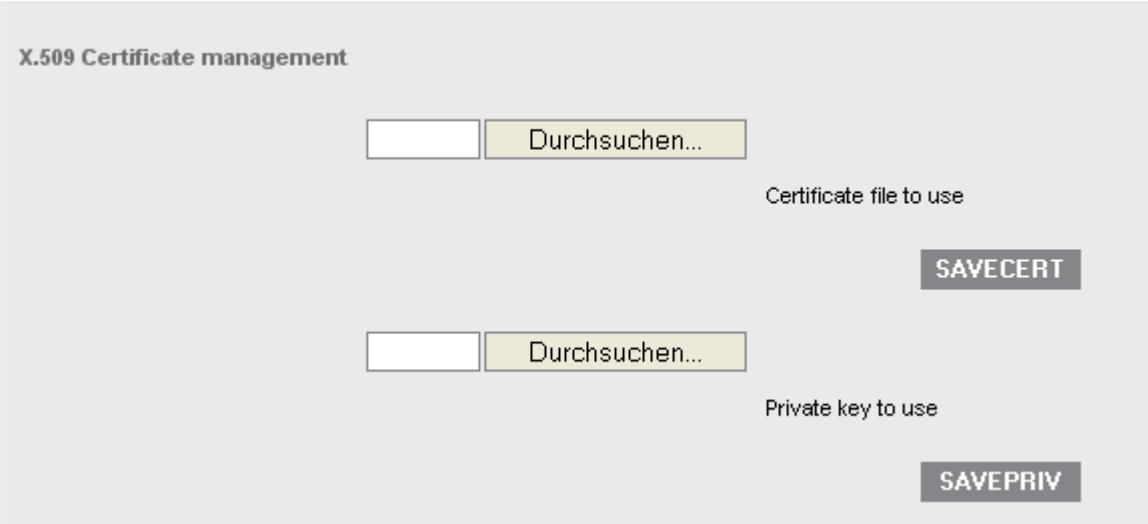
Passwort: preshared key



VPN-ipsec Zertifikate Verbindungen erstellen & verwalten

Grundeinstellung wie unter VPN mit preshared Keys.

Der HY-LINE Router verwendet x.509 Zertifikate. Diese müssen dem Router als 2 getrennte Dateien übergeben werden: die eigentliche Zertifikat Datei (Endung .crt) und die Private Key Datei (Endung nach Typ, z.B. p12 für pkcs 12 Dateien). Liegt das x.509 Zertifikat als eine Datei vor, muß sie - zum Beispiel mit der Software XCA - in 2 Dateien getrennt werden. Das Private Key File darf nicht durch ein Passwort geschützt sein. Falls doch, muß dieses entfernt werden mit OpenSSL.



Aufschlüsseln des Zertifikates in 2 Dateien mit der Software XCA (http://xca.hohnstaedt.de/?page_id=3)

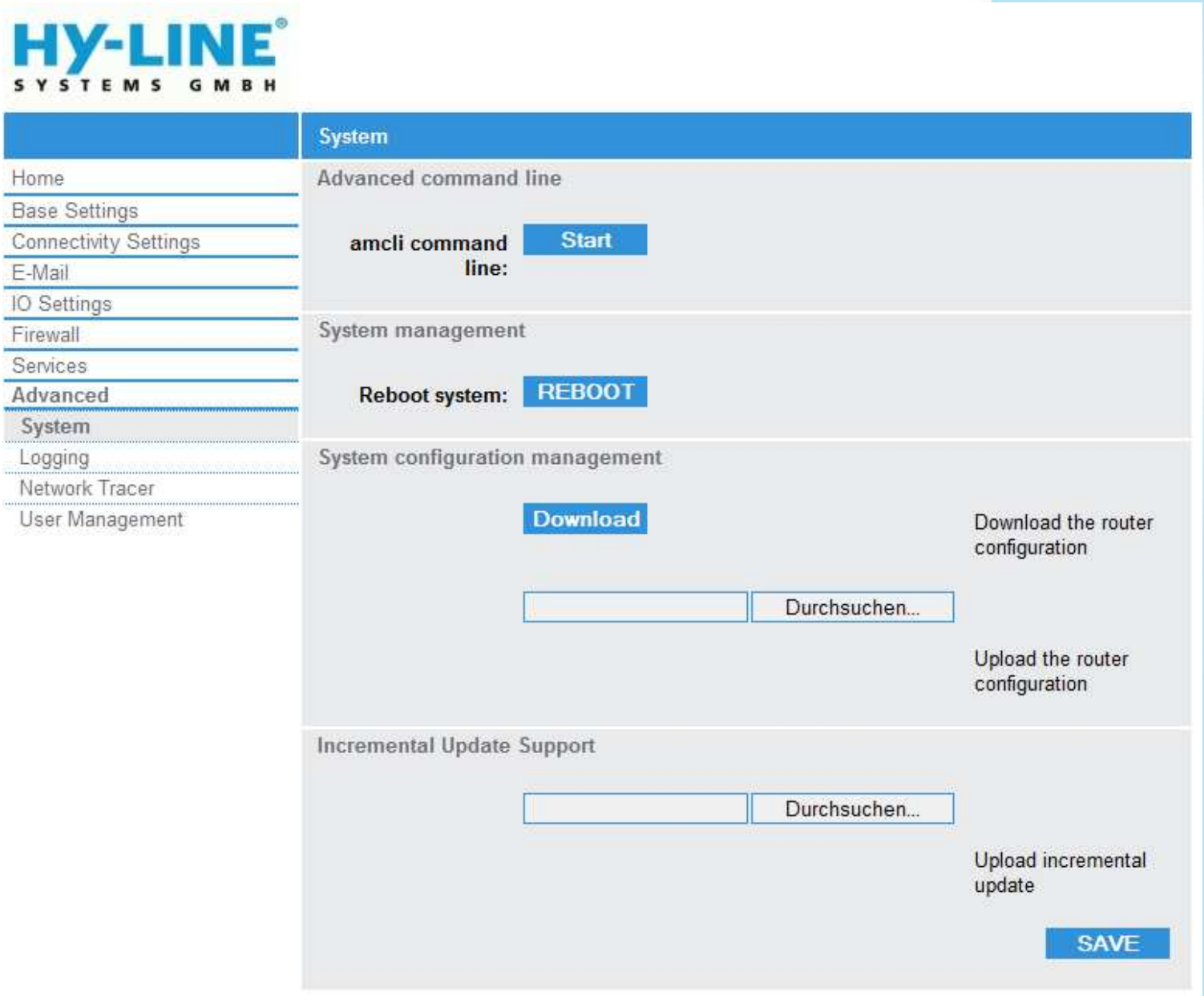
Entfernen des Passworts in der Public Key Datei mit OpenSSL (http://www.openssl.org/):

OpenSSL Kommandozeile starten

Informationen zum Zertifikat (werden diese angezeigt, ist kein Passwort vorhanden):
pkcs12 -in Name_des_Zertifikats.p12 -info

Passwort aus dem Private Key File löschen:
pkcs12 -in Name_des_Zertifikats.p12 -info -nodes -nocerts -out Name_des_Zertifikats _neu.pem

Advanced - System:

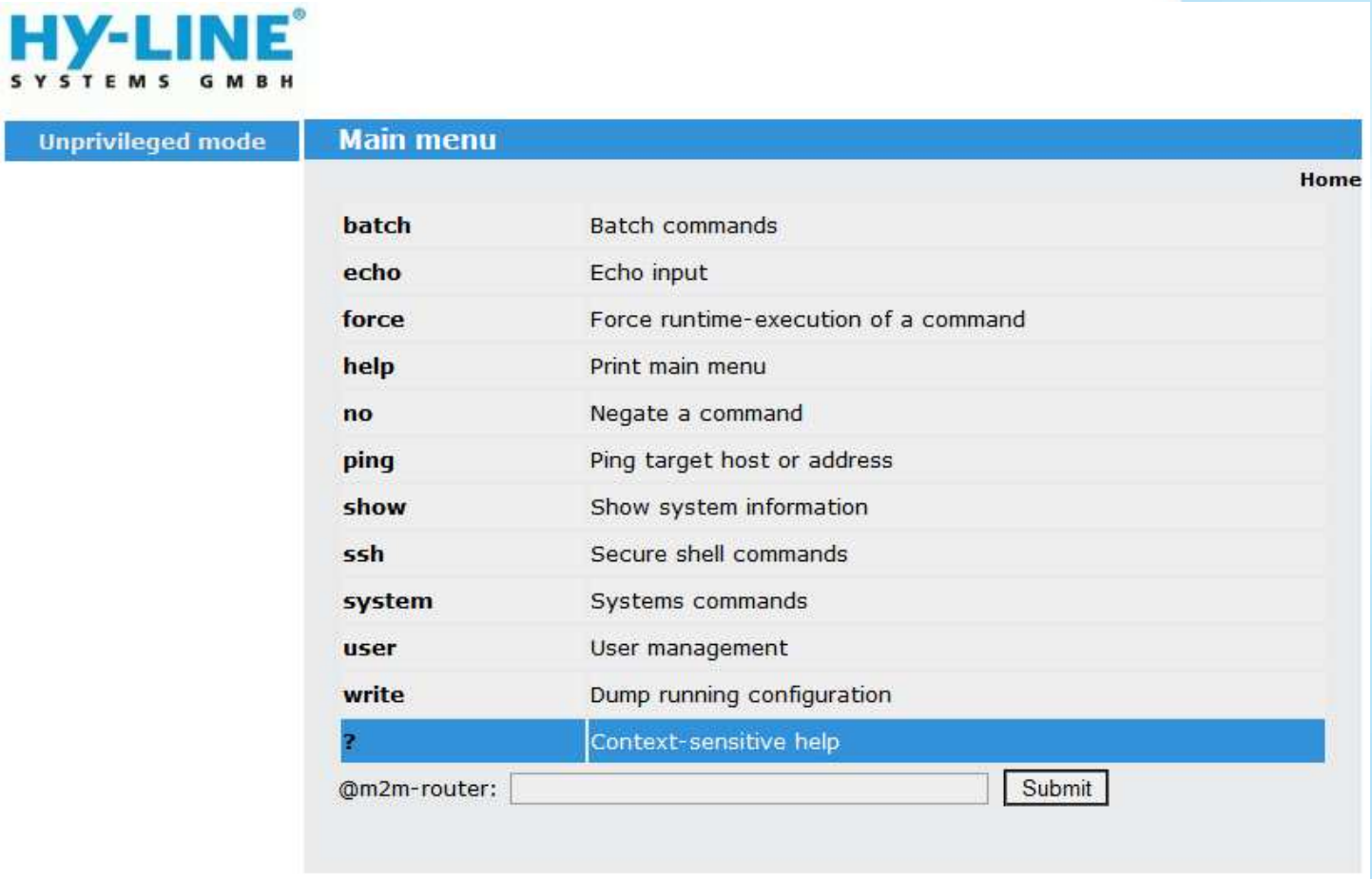


System management:

- **Advanced command line:** Linux-Kommandozeileninterface

Advanced - System:

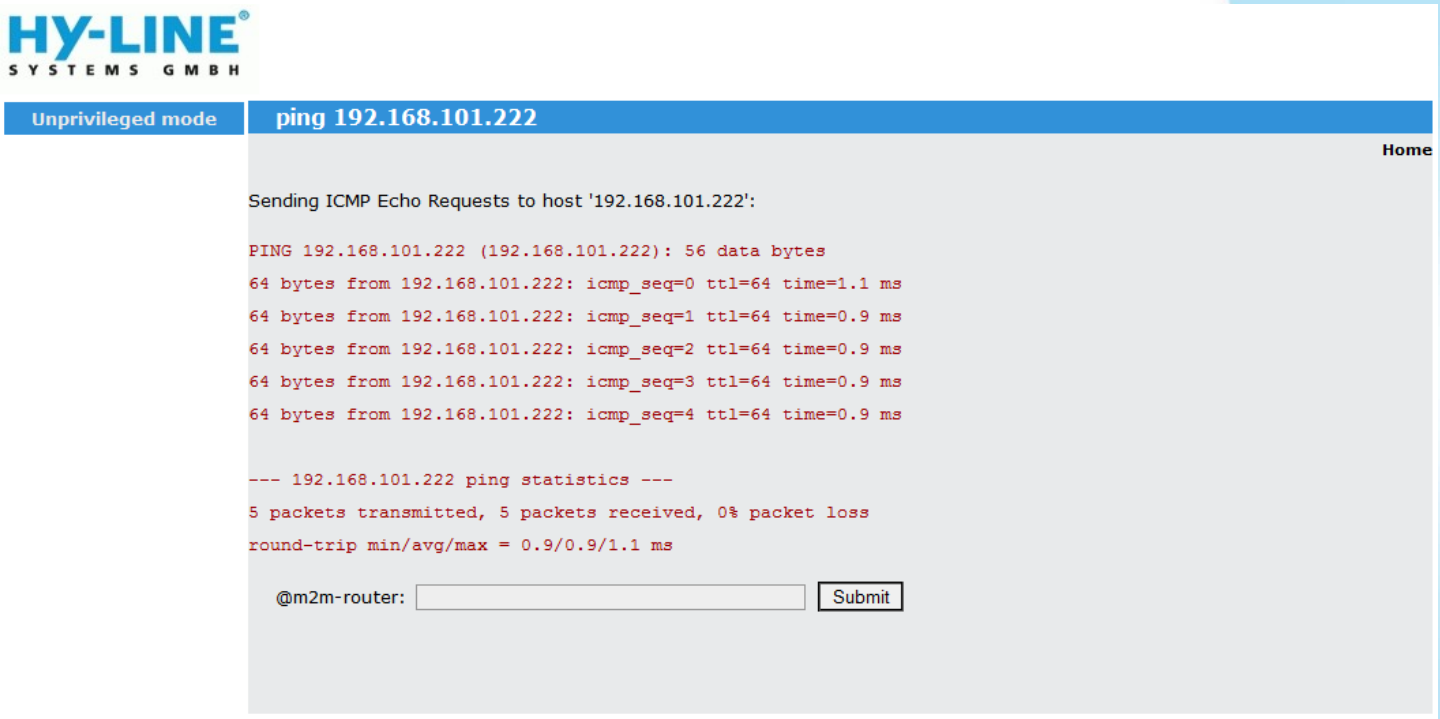
- **Amcli command line:** Die **amcli** ist ein einfaches Kommandozeilen-Interface



Die Parameter für amcli sind durch die Eingabe von amcli -h in der Shell abrufbar.

-c führt die Kommandos aus und beendet das Programm
-d schreibt die Konfiguration und beendet das Programm
-f <file> spezifiziert die Konfigurtionsdatei
-g startet den CGI-Modus
-h zeigt die Hilfe an
-i lässt die init Jobs laufen und beendet das Programm
-m modifiziert die Konfiguration und beendet das Programm
-p löscht die Nodes in der Konfiguration
-r <runlevel> setzt das init Runlevel auf <runlevel>
-s shutdown Modus für init
-v veranlasst das Programm mehr Statusinformationen auszugeben
-D gibt die Konfiguration auf STDOUT aus und beendet das Programm
-F forciertes Initialisieren (bricht bei einem Fehler ab)
-R <file> liest amcli Kommandos aus der Datei <file> aus
-V testet die Konfigurationsdatei auf ihre Richtigkeit und beendet das Programm

- **Amcli command line:** Kommandozeileninterface


HY-LINE
SYSTEMS GMBH
Unprivileged mode
ping 192.168.101.222
Home
Sending ICMP Echo Requests to host '192.168.101.222':
PING 192.168.101.222 (192.168.101.222): 56 data bytes
64 bytes from 192.168.101.222: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 192.168.101.222: icmp_seq=1 ttl=64 time=0.9 ms
64 bytes from 192.168.101.222: icmp_seq=2 ttl=64 time=0.9 ms
64 bytes from 192.168.101.222: icmp_seq=3 ttl=64 time=0.9 ms
64 bytes from 192.168.101.222: icmp_seq=4 ttl=64 time=0.9 ms
--- 192.168.101.222 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.9/0.9/1.1 ms
@m2m-router:
Submit

Ausgabe nach Eingabe eines ping Befehls

Advanced - System:

System management:

- **Reboot system:** Router (Software) Neustart

System configuration management:

- **Download:** Abspeichern der aktuellen Konfiguration des Routers in eine Datei (system.conf). Benutzerrechte beachten unter: ..\Advanced\User Management

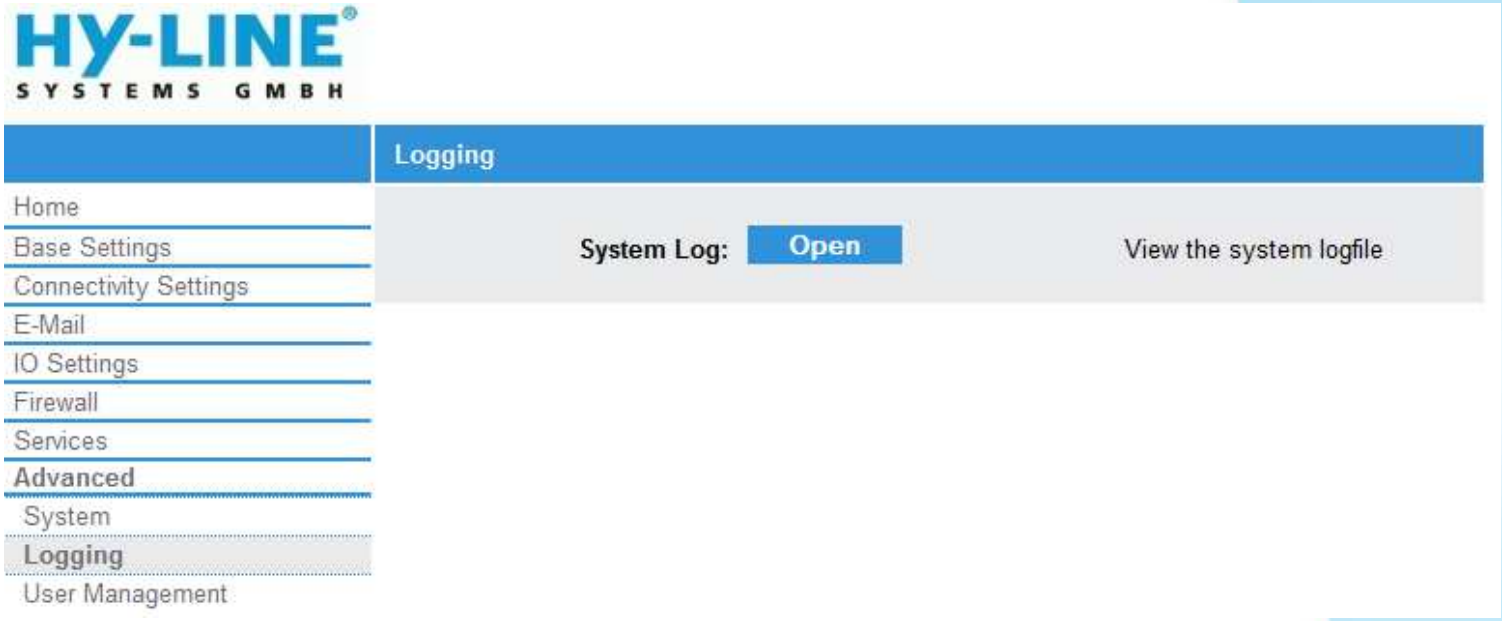
- **Upload:** Laden einer Konfiguration in den Router, nach Upload ist ein Router Neustart erforderlich
→ es dürfen nur Konfiguration gleicher Firmware in Router eingespielt werden!

Wichtiger Hinweis: Der Download und Upload funktioniert nur einwandfrei mit Mozilla Firefox Internet Browser / Safari Browser oder Internet Explorer ab Version 7.x. Die Browser dürfen keine direkte Dateizuordnung zum öffnen von *.conf Dateien haben. Falls die system.conf Datei im Browser direkt geöffnet wird, also kein Download angeboten wird, diese Zuordnung löschen.

- **Incremental Update Support:**

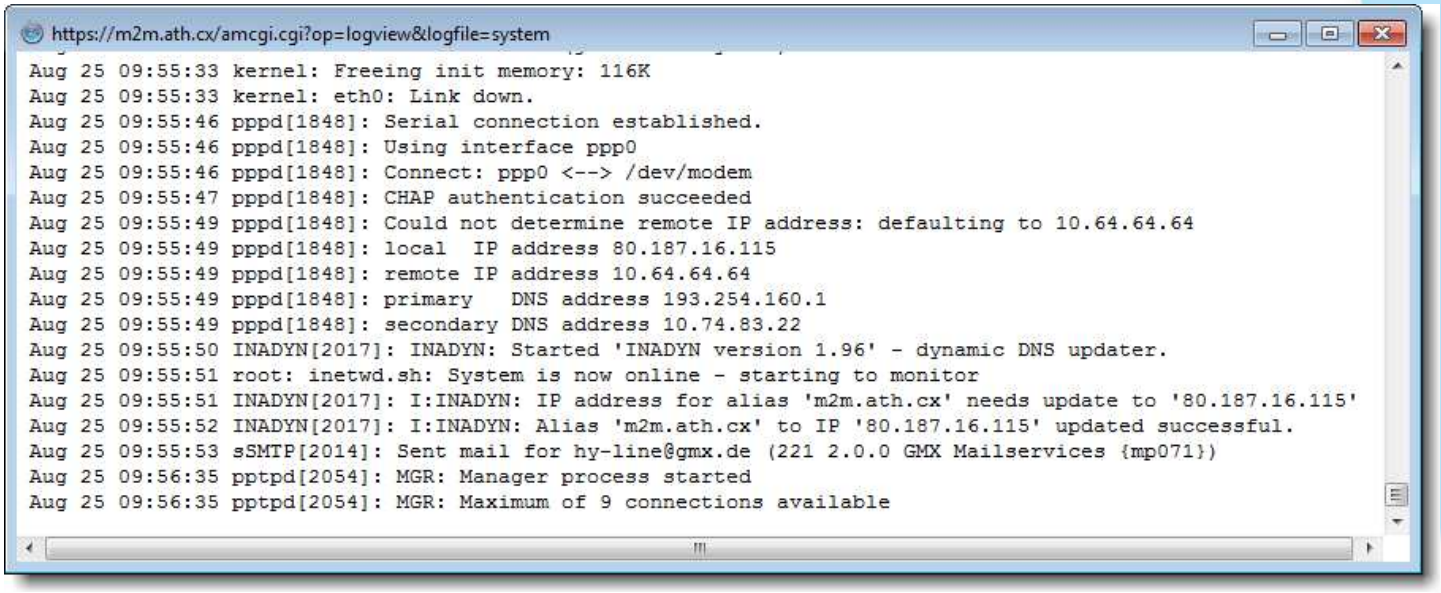
Einspielen von Patches in den Router. Die Patches/Updates werden bei Bedarf vom HY-LINE Support zur Verfügung gestellt.

Advanced - Logging:



- **System Log** zur Router Funktions- und Fehleranalyse

Beispiel Logfile:

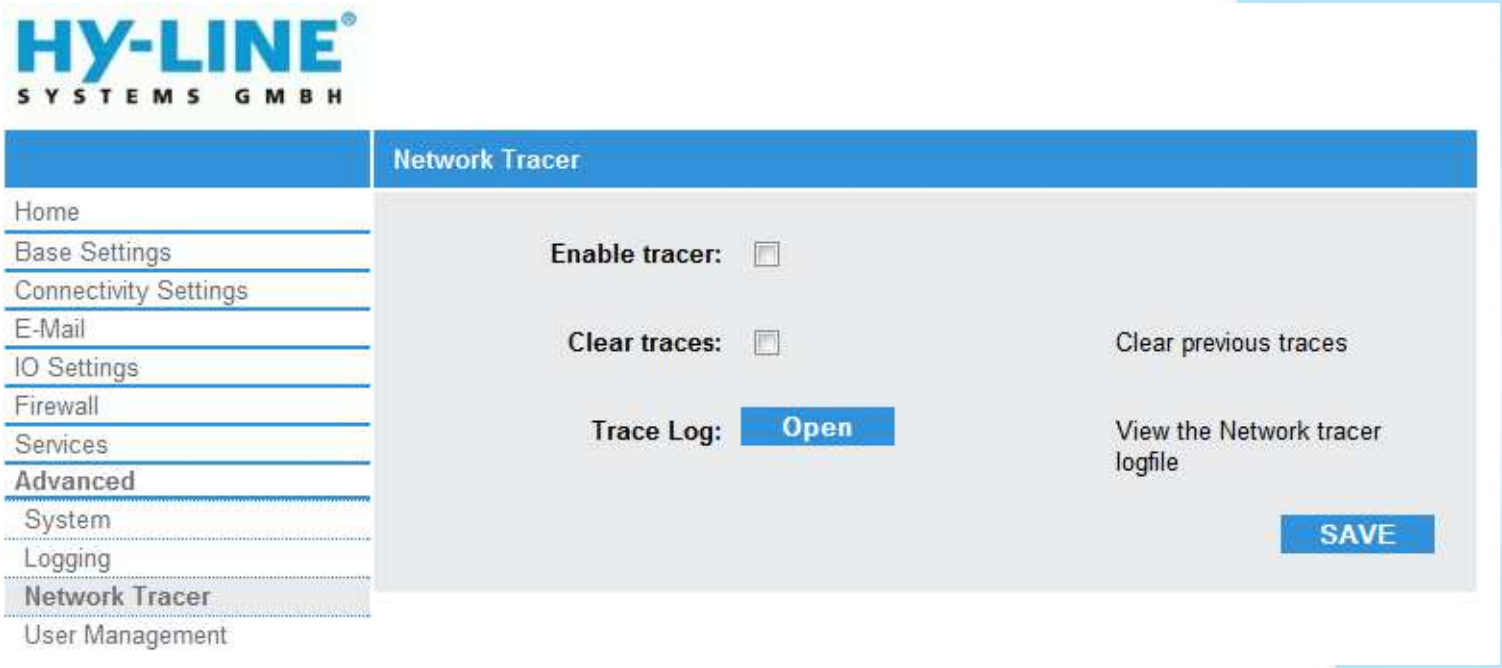

https://m2m.ath.cx/amcgi.cgi?op=logview&logfile=system
Aug 25 09:55:33 kernel: Freeing init memory: 116K
Aug 25 09:55:33 kernel: eth0: Link down.
Aug 25 09:55:46 pppd[1848]: Serial connection established.
Aug 25 09:55:46 pppd[1848]: Using interface ppp0
Aug 25 09:55:46 pppd[1848]: Connect: ppp0 <--> /dev/modem
Aug 25 09:55:47 pppd[1848]: CHAP authentication succeeded
Aug 25 09:55:49 pppd[1848]: Could not determine remote IP address: defaulting to 10.64.64.64
Aug 25 09:55:49 pppd[1848]: local IP address 80.187.16.115
Aug 25 09:55:49 pppd[1848]: remote IP address 10.64.64.64
Aug 25 09:55:49 pppd[1848]: primary DNS address 193.254.160.1
Aug 25 09:55:49 pppd[1848]: secondary DNS address 10.74.83.22
Aug 25 09:55:50 INADYN[2017]: INADYN: Started 'INADYN version 1.96' - dynamic DNS updater.
Aug 25 09:55:51 root: inetwd.sh: System is now online - starting to monitor
Aug 25 09:55:51 INADYN[2017]: I:INADYN: IP address for alias 'm2m.ath.cx' needs update to '80.187.16.115'
Aug 25 09:55:52 INADYN[2017]: I:INADYN: Alias 'm2m.ath.cx' to IP '80.187.16.115' updated successful.
Aug 25 09:55:53 sSMTP[2014]: Sent mail for hy-line@gmx.de (221 2.0.0 GMX Mailservices (mp071))
Aug 25 09:56:35 pptpd[2054]: MGR: Manager process started
Aug 25 09:56:35 pptpd[2054]: MGR: Maximum of 9 connections available

09:55:49: Internet Einwahl und Zuweisung der öffentlichen IP: 80.187.16.115

09:55:50: DynDNS Alias Name Update

09:55:53: E-Mail versand der IP-Adresse

Advanced – Network Tracer:



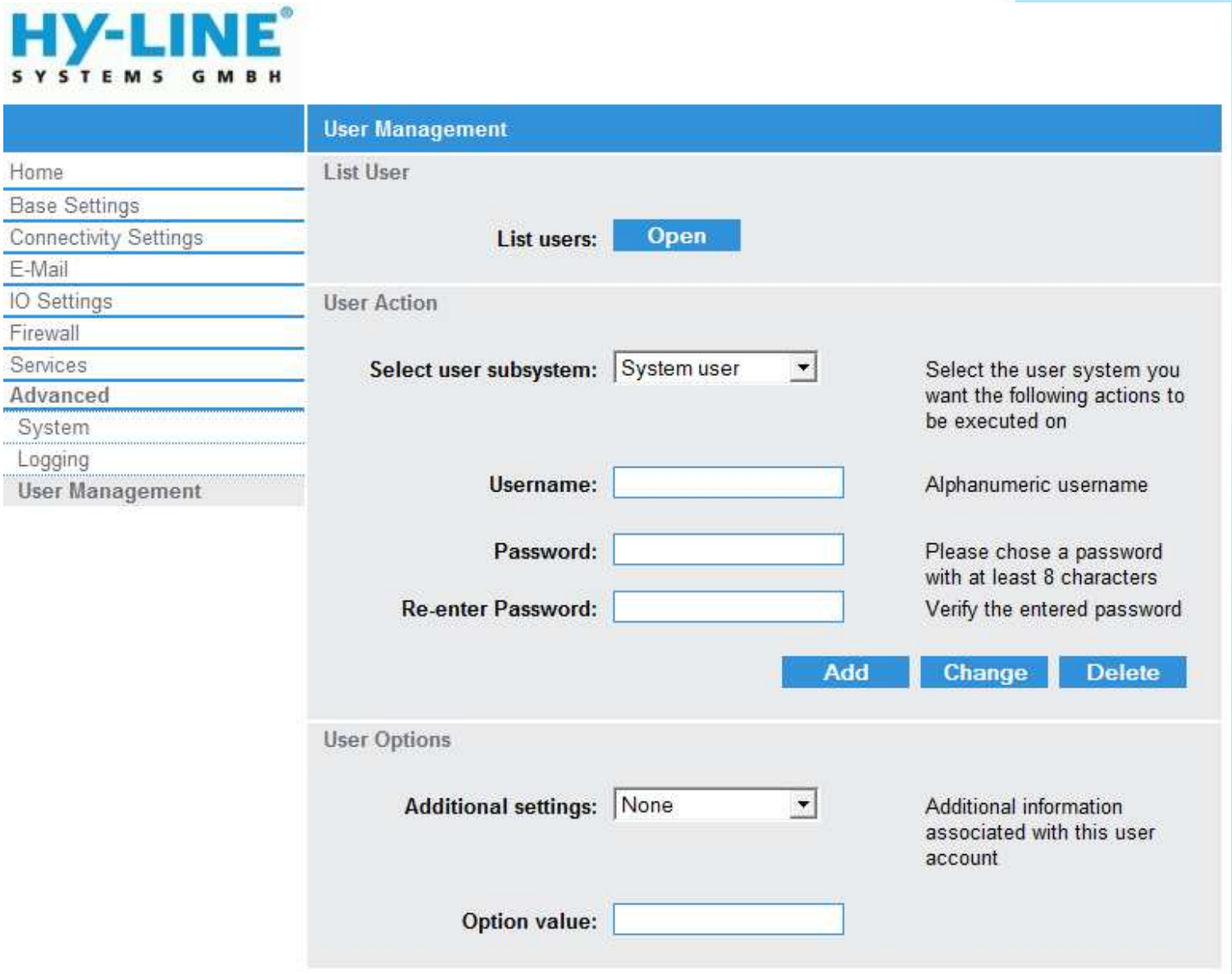
Der **Network tracer** loggt nach dem Aktivieren automatisch den gesamten Netzwerktraffic über alle Schnittstellen. Ausgenommen folgenden Traffic über: Port 22 (ssh), 80 (http), 443 und die vom Router selbst auf diesen Ports generiert werden

- **Enable tracer:** Einschalten des Tracers.
- **Clear traces:** Die aufgezeichneten Logs werden gelöscht.
- **Trace log:** Aufgezeichnetes Log anzeigen.

```
Jan  1 02:21:53 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:22:13 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:22:33 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:22:53 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:23:13 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:23:33 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:23:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:24:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:24:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:24:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:25:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:25:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:25:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:26:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:26:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:26:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:27:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:27:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:27:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:28:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:28:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:28:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:29:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:29:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:29:40 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:8c:73:6e:07:41:2b:08:00 SRC=192.168.101.6 DST=192.168.101.255 LEN=234 TOS=0x00 PREC=0x00 TTL=128 ID=10632 PROTO=UDP SPT=138 DPT=138 LEN=214
Jan  1 02:29:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:30:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:30:32 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:30:52 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
Jan  1 02:31:12 kernel: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:04:00:21:7a:0e:08:00 SRC=192.168.101.55 DST=255.255.255.255 LEN=76 TOS=0x00 PREC=0x00 TTL=254 ID=0 DF PROTO=UDP SPT=10243 DPT=123 LEN=56
```

Beispiel: Tracelog

Advanced - User Management:



User Management:
Über dieses Menü werden neue Benutzer auf dem Router angelegt, bearbeitet und gelöscht.

Bitte beachten:
Es werden *keine* Sonderzeichen in Benutzernamen und Kennwörtern unterstützt!

Advanced - User Management:

- Auf dem Router sind folgende Benutzer mit den entsprechenden **Benutzerrechten**, siehe Tabelle, angelegt:

  - Benutzername: *manager* Passwort: *changemetoo*
  - Benutzername: *service* Passwort: *changemetoo*
  - Benutzername: *installer* Passwort: *changemetoo*
  - Benutzername: *user* Passwort: *changemetoo*

Die angegebenen Rechte laut Tabelle hängen explizit an den Namen der Benutzer. Die Benutzernamen können nicht geändert werden. Die Passwörter können im Menü ‚User Management' geändert werden. Weiter können im gleichen Menü weitere User angelegt bzw. gelöscht werden.

Im Menü ‚List users' werden nur die Benutzer "gleich oder unterhalb" des aktuell angemeldeten Benutzers angezeigt.

User facility	User name	Description
System user		
	root	Admin User
VPN PPTP user		
VPN IPSec user		
Webserver user		
	manager	Web-GUI manager
	service	Web-GUI service
	installer	Web-GUI installer
	user	Web-GUI user
Callback user		

- **Benutzerrechte**

	Webinterface																						
Benutzer	Home	Base Settings	Connectivity Settings	Email	IO Settings	Firewall			Services											Advanced			
						Services	NAT	Status	DHCP Server	DynDNS	Inetwd	NTPd	Ser2TCP	SNMPd	SSHd	Syslogd	UDP Proxy	VPN	WebServer	System	Network Tracer	Logging	User Management *
manager	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
service	+	+	+	+	+	+	+	+	+	+	0	0	-	-	0	0	0	0	0	0	+	+	+
installer	+	+	+	+	+	0	+	0	0	+	0	-	-	-	-	-		0	-	0	+	+	+
user	+	0	-	-	-	-	0	0	-	-	-	-	-	-	-	-		-	-	-	-	+	-

keine Einschränkung
nur schauen
gesperrt

* nur User eigener und darunterliegender Rollen sichtbar

Technische Daten

Technische Daten	
Prinzip	M2M Industrie Router mit freier Modemwahl, VPN und Firewall zur einfachen, sicheren und globalen Kommunikation zu Anlagen und Maschinen.
Router-Version	Analog 56 KBit/s, ISDN 64 KBit/s (Euro-ISDN), GSM/GPRS/EDGE/UMTS/LTE (optional: Mimo/Diversity) Quad-band; DSL; DSL DSL (Annex B/J, optional Annex A) - ADSL, ADSL2 und ADSL2+; LAN-Router - ohne Modem
VPN	Virtual Private Network, Protokolle: OpenVPN Client und Server, IPSec (Pre-Shared Key/X.509 Zertifikate); PPTP (PAP, CHAP, MS-CHAP V2)
PPP	Point to Point Protokoll, Analog/ISDN und GSM-Modembetrieb, unterstützt Call-back Funktionalität
PPPoE	Point to Point over Ethernet Protokoll, unterstützt den Anschluss von ext. Modems über Ethernet/PPPoE
Firewall	NAT, Port Forwarding, Paket- und Port-Filter
Services	DynDNS, DHCP/DNS Server, SNMP, NTP, SMTP, FTP
Konfig./Management	Integrierter HTML-Webserver, HTTP, HTTPS, SSH, Seriell
Alarmierung	E-Mail, SMS, über digitale Schalteingänge triggerbar
Digitale Schalteingänge	2 x 5-30 VDC/VAC, Schaltstrom min. 5 mA, konfigurierbar als potenzialfreie Eingänge
Digitaler Schaltausgang	24V DC / max. 100 mA, Kurzschlussfest
Schnittstellen	Ethernet RJ45, 10/100Mbit/s; RS232-DSUB-9; analog RJ11; ISDN RJ45; DSL RJ45; Antennenbuchsen: FME (male), optional: SMA (female)
Status LEDs	Betrieb, Netzwerk, Online, Digitale Eingänge 1+2, Digitalausgang
Umweltbedingungen	Analog-Router, ISDN-Router: Betrieb 0°C bis +70°C GSM/GPRS/UMTS/LTE-Router: Betrieb -20°C bis +70°C DSL-Router: Betrieb 0°C bis +50°C (optional: -20°C bis +70°C) LAN-Router, ohne int. Modem: Betrieb -20°C bis +70°C Alle Varianten: Luftfeuchtigkeit: 0-95%, nicht kondensierend
Spannungsversorgung	12-30 VDC, Leistungsaufnahme: max. 3-5 Watt, abhängig von Router-Variante
Zulassungen	CE, EMV nach EN61000-4-3, EN61000-4-2, ENV50204, EN55022-B
Gehäuse	120 x 101 x 35 mm, ca. 250 g, Kunststoff Hutschienengehäuse IP 20
Lagertemperaturbereich:	Analog-Router: -40°C bis +85°C ISDN-Router: -10°C bis +85°C GSM/GPRS/UMTS/LTE-Router: -40°C bis +85°C DSL-Router: -30°C bis +75°C LAN-Router, ohne int. Modem: -50°C bis +85°C

Technische Daten: Router mit integriertem 4-fach Switch

Daten wie bei Standard-Router (siehe Seite 71), mit folgenden Änderungen/Zusätzen:

Wichtig: die einzelne Netzwerkbuchse RJ45 auf der Seite des Routers ist bei der Router Version mit integriertem Switch nicht belegt und darf nicht verwendet werden. Diese ist im Auslieferzustand mit einem Blindstopfen versiegelt. Dieser darf nicht entfernt werden.

Technische Daten: Router mit integriertem 4-fach Switch	
Ethernet-Schnittstellen	Integrierter 4-fach 10/100 Mbit/s Base-T, Ethernet RJ45 Switch auf der Frontseite, Auto Negotiation, Auto Crossing, Auto Polarity Status-LEDs: Funktion, Link, Speed Trennspannung: 1000VAC Ethernet und Versorgungsspannung IEEE 802.3 (CSMA/CD), IEEE 802.3ux (Fast Ethernet, Full Duplex Mode)
Spannungsversorgung	12-30 VDC, Leistungsaufnahme: max. 4-6 Watt, abhängig von Router-Variante
Zulassungen	CE, EMV nach EN61000-4-3, EN61000-4-2, ENV50204, EN55022-B
Gehäuse	120x100x60mm (83mm DSL-Version) ca. 250g, Kunststoff Hutschienengehäuse, IP20

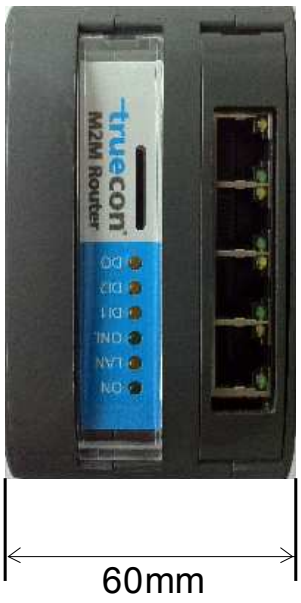
Abb.: HY-LINE Router mit integr. 4-fach Switch

Abmessungen

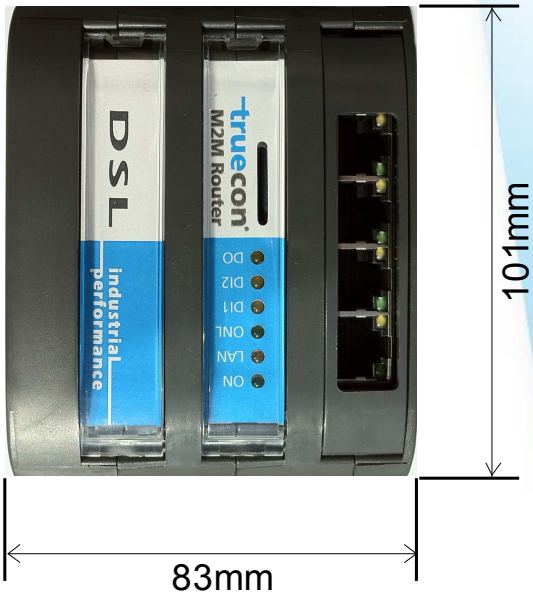
Gehäuse zur Montage auf Tragschiene nach DIN (EN 60715), Kunststoff, IP 20

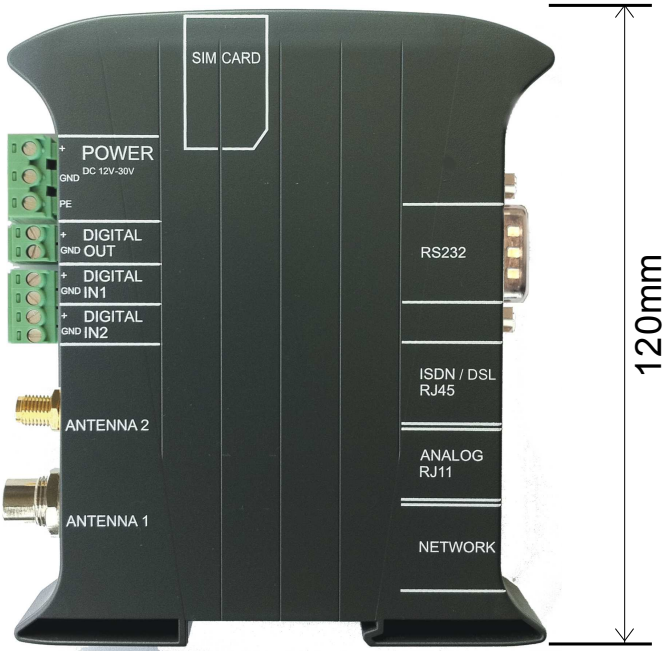
HAP-R
HAP-RI
HAP-RA
HAP-RG
HAP-RU
HAP-RL

HAP-RS
HAP-RIS
HAP-RAS
HAP-RGS
HAP-RUS
HAP-RLS



HAP-RDS





Ländereinstellung Analog-Router:

- Einloggen über SSH oder seriell:

- Folgende Befehle eintippen (unbedingt auf Groß-Kleinschreibung achten!):

```
sys sh

svactivate stop mgetty-s0

svactivate stop pppd

microcom /dev/ttyS0
```

`at+gci=42` (=Germany) oder nach untenstehender Liste, z.B. United Kingdom= B4

```
at&w
```

- Router rebooten

2.2.3 Worldwide Operation

The modem operates in TBR21-compliant and other countries. Country-dependant modem parameters for functions such as dialing, carrier transmit level, calling tone, call progress tone detection, answer tone detection, blacklisting, caller ID, and relay control are programmable. Country code IDs are defined by ITU-T T.35.

The default countries supported are:

Country	Country Code	Country	Country Code	Country	Country Code
Australia	09	India	53	Portugal	8B
Austria	0A	Ireland	57	Singapore	9C
Belgium	0F	Italy	59	South Africa	9F
Brazil	16	Japan	00	Spain	A0
China	26	Korea	61	Sweden	A5
Denmark	31	Malaysia	6C	Switzerland	A6
Finland	3C	Mexico	73	Taiwan	FE
France	3D	Netherlands	7B	United King.	B4
Germany	42	Norway	82	United States	B5
Greece	46	Poland	8A		

Versorgungsspannung / Leistungsaufnahme:

Der HY-LINE Router kann von 12-30 VDC betrieben werden. Die Leistungsaufnahme ist abhängig von der Betriebsspannung. Eine pauschale Aussage, wie die Leistungsaufnahme abhängig zur Betriebsspannung ist, kann man aus technischer Sicht nicht so einfach machen.

Folgendes gilt:

- je niedriger die Versorgungsspannung eines Gerätes wird, je höher wird die Stromaufnahme und je schlechter wird der Wirkungsgrad des internen Spannungswandlers

- Beispiel: Versorgungsspannung: 24 VDC, Stromaufnahme: 100mA, Leistungsaufnahme: 2.4W, Wirkungsgrad: relativ 1 (technisch nicht möglich, aber einfacher zur Anschauung)

- Beispiel: Versorgungsspannung: 12 VDC, Stromaufnahme: 235mA, Leistungsaufnahme: 2.82W, Wirkungsgrad: 0.85

Als **Fazit** kann angenommen werden: Bei Halbierung der Versorgungsspannung verdoppelt sich die Stromaufnahme (+15%) und somit steigt die Leistungsaufnahme auch um ca. 15%

- **Alle Werte sind Maximalwerte, falls nicht anders angegeben!**
- **Betriebsspannung: 24VDC**
- **Router mit integrierten 4-fach Switch erhöhen den Strombedarf um 40mA permanent**

HAP-RI ISDN-Router: ***max: 1.80W***

Bootvorgang: 65mA
Webseiten laden: 73mA
Digitale I/OS schalten: 70mA
Online/Sende-Empfangsbetrieb: 65mA

HAP-RA Analog-Router: ***max: 1.95W***

Bootvorgang: 75mA
Webseiten laden: 76mA
Digitale I/OS schalten: 79mA
Online/Sende-Empfangsbetrieb: 72mA

HAP-RG GSM/GPRS-Router: ***max: 2.70W***

Bootvorgang: 100mA
Webseiten laden: 88mA
Digitale I/OS schalten: 65mA
Online/Sende-Empfangsbetrieb: 100mA

HAP-RU UMTS/LTE-Router: ***max: 3.6W***

Bootvorgang: 150mA
Webseiten laden: 150mA
Digitale I/OS schalten: 100mA
Online/Sende-Empfangsbetrieb: 80mA

HAP-RDS DSL-Router: ***max: 7.5W***

Bootvorgang: 300mA
Webseiten laden: 300mA
Digitale I/OS schalten: 300mA
Online/Sende-Empfangsbetrieb: 300A

SMS senden direkt vom truecon M2M Router

Das Versenden von SMS-Meldungen erfolgt über den E-Mailer und über die Möglichkeit mit einem Handy E-Mails zu empfangen. Jeder Mobilfunkprovider bietet Ihnen diese Funktion an.
Achtung: die SMS wird vom Empfänger bezahlt! Kosten hierfür bitte beim jeweiligen Mobilfunkbetreiber erfragen!

Schalten Sie Ihr Handy entsprechend den Angaben Ihres Providers für E-Mails frei. Sie erhalten dann automatisch eine E-Mail Adresse für Ihr Handy. In den meisten Fällen lautet die Adresse Telefonnummer@Providername.de (z.B. Handy-Nummer@d2-mobil.de).

Der Versand von SMS-Nachrichten wird durch die Verwendung von speziellen Gateways der Telefondienstanbieter erreicht. Eine SMS an eine D2 Handy-Nummer wird zum Beispiel mit einer E-Mail an folgende Adresse erzeugt: Handy-Nummer@d2-message.de.

Der Empfang von E-Mails als SMS auf einem Handy ist kostenpflichtig. Daher müssen Sie diesen Dienst bei Ihrem Moblilnetzbetreiber aktivieren.

Die folgende Liste zeigt, wie Sie das Empfangen von E-Mail auf einem Mobiltelefon aktivieren und deaktivieren. Bitte fragen Sie ggf. die aktuellen Einstellungen beim Provider nach.

D1: E-Mailadresse: Handy-Nummer@t-d1-sms.de Aktivieren: SMS "open" an Tel.Nr. 8000 Deaktivieren: SMS "close" an Tel.Nr. 8000

D2: E-Mailadresse: Handy-Nummer@d2-message.de Aktivieren: SMS "open" an Tel.Nr. 3400 Deaktivieren: SMS "close" an Tel.Nr. 3400
Voraussetzung ist der Dienst D2MessagePlus mit der SMS-Zentrale 2270333

e-Plus: E-Mailadresse: Handy-Nummer@smsmail.eplus.de Aktivieren: SMS "start" an Tel.Nr. 7676245 Deaktivieren: SMS "stop" an Tel.Nr. 7676245

T-Mobile (D1)

- Empfang aktivieren: SMS mit Text '**OPEN**' an '**8000**' senden.
- Empfang sperren: SMS mit Text '**CLOSE**' an '**8000**' senden.
- Email-Adresse: **handynummer@t-mobile-sms.de**

Vodafone (D2)

- Empfang aktivieren: SMS mit Text '**OPEN**' an '**3400**' senden.
- Empfang sperren: SMS mit Text '**CLOSE**' an '**3400**' senden.
- Email-Adresse: **handynummer@vodafone-sms.de**

E-Plus

- Empfang aktivieren: SMS mit Text '**START**' an '**7676245**' senden.
- Empfang sperren: SMS mit Text '**STOP**' an '**7676245**' senden.
- Email-Adresse: **handynummer@smsmail.eplus.de**

o2 Germany

- Empfang aktivieren: SMS mit Text '**+OPEN**' an '**6245**' senden.
- Empfang sperren: SMS mit Text '**STOP**' an '**6245**' senden.
- Email-Adresse: **handynummer@o2online.de**

Konfiguration des (GPRS/UMTS/LTE) M2M Router bei Betrieb mit VPN-PPTP und DynDNS:

Hinweis: Jede Einstellung muß mit der SAVE-Schalfläche auf der jeweiligen Seite bestätigt werden, am Ende der Konfiguration muß der M2M Router neu gebootet werden.

Grundeinstellung:

- Router spannungslos schalten, SIM-Karte in Router einstecken, Router einschalten

- im Menü \Base Settings\Network\ die IP Einstellungen auf Ihre IT-Infrastruktur anpassen (es darf hier kein Gateway eingetragen werden)

- im Menü \Connectivity Settings\Base Settings\ die PIN der SIM Karte eintragen und PIN enablen (falls SIM Karte durch Pin geschützt ist)

- im Menü \Connectivity Settings\Internet Settings\ den ISP: GPRS-GSM wählen, auf Set+Save klicken und ggfs. die Einwahldaten ihrer SIM-Karte anpassen (APN, Benutzername und Passwort). Falls gewünscht, hier das DynDNS Protokoll (unter IP reporting mode) aktivieren

- im Menü \Connectivity Settings\Dial In\ die Call back Einstellung auf 5 Rings einstellen

- im Menü\Services\DHCP\ die IP-Range auf Ihre Infrastruktur anpassen (nur notwendig bei Verwendung des Router als DHCP Server), ansonsten DHCP Server deaktivieren

VPN-PPTP Server Einstellung:

- im Menü \Services\VPN Services\ den PPTP Server aktivieren (use PPTP daemon)

- im Menü \ Services\VPN\PPTP\Server\ die Client - und Server IP so anpassen, das diese nicht in Ihrer IT-Netzwerk Infrastruktur vorkommen (VPN-Tunnel muß mit 'einzigartigen' IP-Adressen aufgebaut werden)

- im Menü \Advanced\User Management\ einen neuen User anlegen: User Subsystem: PPP/PPTP User

DynDNS Einstellung:

- im Menü \Services\DynDNS\ hier die Daten zum DynDNS eintragen (Benutzername und Passwort zum Einloggen am DynDNS Server, ALIAS Name für den M2M Router)

Einstellungen der Geräte im Router Anlagennetz:

- in diesen Geräten muß die IP-Adresse des M2M Routers als Gateway eingetragen sein